



WHA-5500CPE

802.11a Multi-Function
Outdoor CPE

User's Manual



www.airlive.com

Declaration of Conformity

We, Manufacturer/Importer

OvisLink Corp.

**5F., NO.6, Lane 130, Min-Chuan Rd.,
Hsin-Tien City, Taipei County, Taiwan**

Declare that the product

802.11a Multi-function Outdoor AP


AirLive WHA-5500CPE

is in conformity with

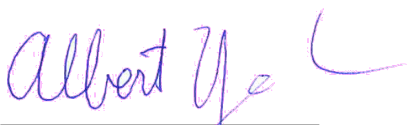
In accordance with 89/336 EEC-EMC Directive and 1999/5 EC-R & TTE Directive

Clause

Description

- | | |
|---|---|
| ■ EN 301 893 v1.3.1
(2005-03) | Broadband Radio Access Network(BRAN); 5GHz high performance RLAN; Harmonized EN Covering essential requirements of Article 3.2 of the R&TTE Directive. |
| ■ EN 300 328 v1.7.1
(2006-10) | Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission equipment operating in the 2.4GHz ISM band And using spread spectrum modulation techniques; Part 1 : technical Characteristics and test conditions Part2 : Harmonized EN covering Essential requirements under article 3.2 of the R&TTE Directive |
| ■ EN 301 489-1 v1.6.1
(2005-09) | Electromagnetic compatibility and Radio spectrum Matters (ERM); |
| ■ EN 301 489-17 v1.2.1
(2002-08) | Electromagnetic compatibility(EMC) standard for radio equipment and Services; Part 17 : Specific conditions for wideband data and HIPERLAN equipment |
| ■ EN 50371:2002 | Generic standard to demonstrate the compliance of low power Electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic field (10MHz – 300GHz)
-General public |
| ■ EN 60950-1:2001 | Safety for information technology equipment including electrical business equipment |
| ■ CE marking |  |

Manufacturer/Importer



Albert Yeh

Vice President

Signature :
Name :
Position/ Title :

Date : **2007/10/4**

(Stamp)

AirLive WHA-5500CPE CE Declaration Statement

Country	Declaration	Country	Declaration
cs Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento AirLive WHA-5500CPE je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.	lt Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruojama, kad šis AirLive WHA-5500CPE atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
da Dansk [Danish]	Undertegnede OvisLink Corp. erklærer herved, at følgende udstyr AirLive WHA-5500CPE overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.	nl Nederlands [Dutch]	Hierbij verklaart OvisLink Corp. dat het toestel AirLive WHA-5500CPE in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
de Deutsch [German]	Hiermit erkläre OvisLink Corp., dass sich das Gerät AirLive WHA-5500CPE in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.	mt Malti [Maltese]	Hawnhekk, OvisLink Corp, jiddikjara li dan AirLive WHA-5500CPE jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 1999/5/EC.
et Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme AirLive WHA-5500CPE vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.	hu Magyar [Hungarian]	Az OvisLink Corporation kijelenti, hogy az AirLive WHA-5500CPE megfelel az 1999/05/CE irányelv alapvető követelményeinek és egyéb vonatkozó rendelkezéseinek.
en English	Hereby, OvisLink Corp., declares that this AirLive WHA-5500CPE is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	pl Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że AirLive WHA-5500CPE jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
es Español [Spanish]	Por medio de la presente OvisLink Corp. declara que el AirLive WHA-5500CPE cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.	pt Português [Portuguese]	OvisLink Corp declara que este AirLive WHA-5500CPE está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ ΟΤΙ AirLive WHA-5500CPE ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK.	sl Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta AirLive WHA-5500CPE v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
fr Français [French]	Par la présente OvisLink Corp. déclare que l'appareil AirLive WHA-5500CPE est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	sk Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že AirLive WHA-5500CPE spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
it Italiano [Italian]	Con la presente OvisLink Corp. dichiara che questo AirLive WHA-5500CPE è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	fi Suomi [Finnish]	OvisLink Corp vakuuttaa täten että AirLive WHA-5500CPE tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen
lv Latviski [Latvian]	Ar šo OvisLink Corp. deklarē, ka AirLive WHA-5500CPE atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.	is Íslenska [Icelandic]	Hér með lýsir OvisLink Corp yfir því að AirLive WHA-5500CPE er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
sv Svenska [Swedish]	Härmed intygar OvisLink Corp. att denna AirLive WHA-5500CPE står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.	no Norsk [Norwegian]	OvisLink Corp erklærer herved at utstyret AirLive WHA-5500CPE er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

A copy of the full CE report can be obtained from the following address:

OvisLink Corp.
5F, No.6 Lane 130,
Min-Chuan Rd, Hsin-Tien City,
Taipei, Taiwan, R.O.C.

This equipment may be used in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LV, LT, LU, MT, NL, PL, PT, SK, SI, ES, SE, GB, IS, LI, NO, CH, BG, RO, TR

Regulatory Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Copyright Statement

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise without the written consent of OvisLink Corp.

Windows™ 95/98 and Windows™ 2000 are trademarks of Microsoft® Corp.

Pentium is trademark of Intel.

All copyright reserved.

Table of Contents

1. Introduction	1
1.1 Overview.....	1
1.2 Features	1
1.3 Wireless Operation Modes	2
1.3.1 Access Point Mode	2
1.3.2 Repeater Mode	3
1.3.3 WDS Bridge Mode	3
1.3.4 Client Infrastructure Mode	4
1.3.5 Client Ad Hoc Mode	4
1.3.6 WISP Router Mode	5
1.4 Set up the device	5
1.4.1 STATIC IP	5
1.4.2 AUTOMATIC IP	6
2. Install the 802.11 A Access Point	7
2.1 What's in the box?	7
2.2 Hardware Installation	8
2.2.1 Mounting Configuration.....	10
2.2.2 Antenna polarization	11
2.3 Configuration steps.....	12
2.4 Set up a wireless client as a DHCP client.....	13
3. Basic Configuration	14
3.1 Setup wizard	15
3.1.1 TIME SETTINGS	15
3.1.2 DEVICE IP SETTINGS	16
3.1.3 WIRELESS SETTINGS	17
3.1.4 FINISH SETUP WIZARD AND SAVE YOUR SETTINGS	23
3.2 Advanced settings.....	24
3.2.1 PASSWORD SETTINGS	24
3.2.2 SYSTEM MANAGEMENT	25
3.2.3 SNMP Settings	26
3.2.4 MAC FILTERING SETTINGS	28
3.2.5 OPERATIONAL MODE	28
3.3 Access Point Mode Settings	30
3.3.1 Wireless Settings	31
3.3.2 SSID Settings	32
3.3.3 QoS Settings	33
3.3.4 RADIUS Settings	34
3.4 Repeater Mode Settings	35

3.4.1 AP Node Settings.....	35
3.4.2 Repeater Node Settings	37
3.4.3 Repeater Node Local service Settings.....	38
3.4.4 Repeater Advance Wireless Setting	38
3.4.5 QoS Settings	40
3.4.6 RADIUS Settings	41
3.5 WDS Bridge Mode Settings	42
3.5.1 Wireless Settings	43
3.6 Client Infrastructure Mode Settings.....	44
3.6.1 Wireless Settings	45
3.7 Client Adhoc Mode Settings.....	46
3.7.1 Wireless Settings	46
3.8 WISP Router Mode Settings	47
3.8.1 Wireless Settings	47
3.8.2 WISP Router DHCP Server Settings	49
3.8.3 Multiple DMZ	50
3.8.4 Virtual Server Settings	51
3.8.5 Special Applications	52
3.8.6 IP Filtering Settings.....	53
3.8.7 IP Routing Settings	54
3.9 ACK Timeout Setup	55
4. Manage the WHA-5500CPE	57
4.1 Device Status.....	57
4.2 System Log.....	58
4.3 Wireless Client Table	58
4.4 Radio Table	59
4.5 Site Survey	59
4.5.1 Signal survey	60
4.6 Firmware Upgrade	61
4.7 Configuration Save and Restore.....	62
4.8 Factory Default	63
4.9 Reboot System	63
4.10 What if you forgot the password?	64
5. Specifications.....	65

1

Introduction

1.1 Overview

The WHA-5500CPE is a wireless access-point based on IEEE 802.11a 5-GHz radio technologies. It contains an 802.11a wireless interface and one half/full-duplex 10/100 LAN interface. Moreover, WHA-5500CPE features a total of 6 wireless modes: Access Point, Repeater, WDS Bridge, Client Infrastructure, Client Ad Hoc and WISP Router.

To address growing security concerns in a wireless LAN environment, different levels of security can be enabled in WHA-5500CPE:

- To disable SSID broadcast to restrict association to only those client stations that are already pre-configured with the correct SSID
- To enable WEP (Wireless Encryption Protocol) 64, 128, or 152-bit encryption to protect the privacy of your data.
- Support of Access List Control to allow you to grant/deny access to/from specified wireless stations
- Provisioning of centralized authentication through RADIUS Server.
- WPA-PSK (Wi-Fi Protected Access, Pre-Shared Key) for home users to provide authentication, data integrity, and data privacy.
- WPA (Wi-Fi Protected Access) works with a RADIUS server to provide stronger authentication as well as data integrity and privacy.

1.2 Features

- Compliant with 802.11a and Super A™ standards with roaming capability.
- Supports 6 wireless multi-function modes: Access Point, Repeater, WDS Bridge, Client Infrastructure, Client Ad Hoc and WISP Router.
- Static assignment or DHCP client to set the device IP address.
- Multiple security measures: SSID hiding, Access Control List, WEP based encryption (64, 128, 152 bits), enhanced Security with 802.1x using a primary and a backup RADIUS Server with/without dynamic WEP keys, WPA-PSK, WPA, and WPA2.
- Extensive monitoring capability such as event logging, traffic/error statistics monitoring. Support of remote logging.
- Easy configuration and monitoring through the use of a Web-browser based GUI, SNMP commands from a remote SNMP management station, and UPnP for users to automatically discover the device.
- Setup Wizard for easy configuration/installation.
- Configuration file download and restore.

- Firmware upgradeable.

1.3 Wireless Operation Modes

A group of wireless stations communicating with each other is called a Basic Service Set (BSS) and is identified by a unique SSID.

When a WHA-5500CPE is used, it can be configured to operate in the following network configurations.

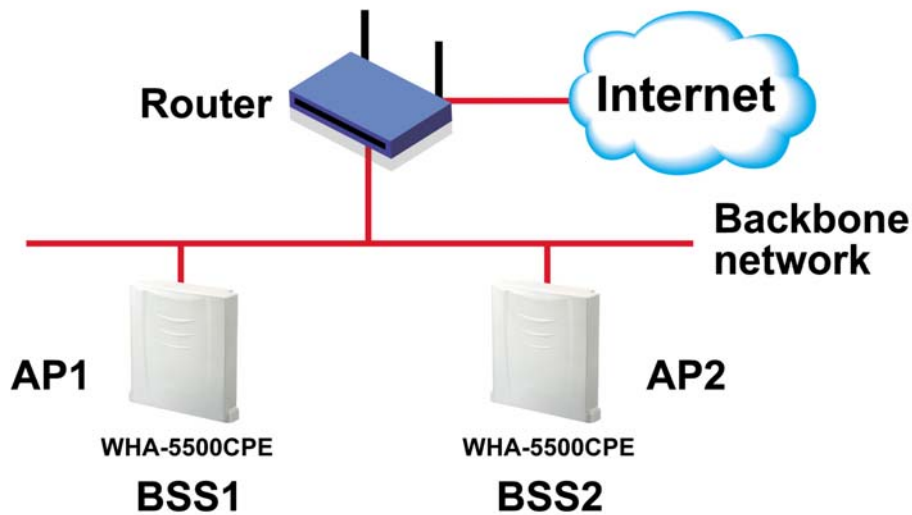
1.3.1 Access Point Mode

When configured in the Access Point mode, the WHA-5500CPE allows a group of wireless stations to communicate with each other through it. Such a network is called an Infrastructure BSS.



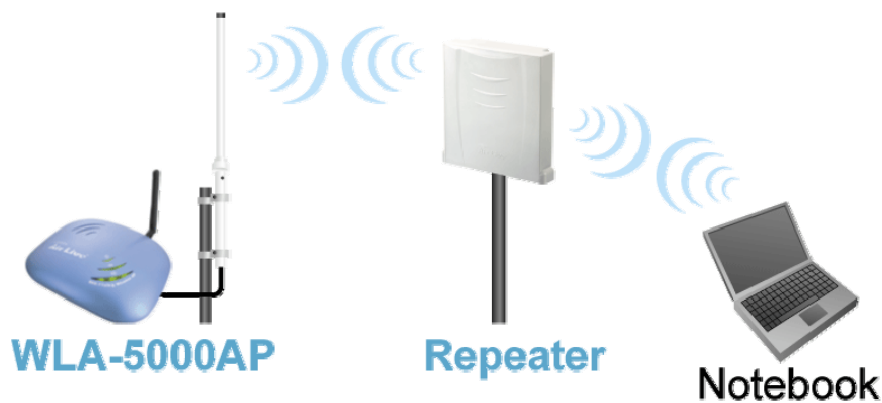
The WHA-5500CPE further provides bridging functions between the wireless network and the wired LAN network.

When multiple access points are connected to the same LAN segment, stations can **roam** from one WHA-5500CPE to another without losing their connections, as long as they are using the same SSID. See the diagram below.



1.3.2 Repeater Mode

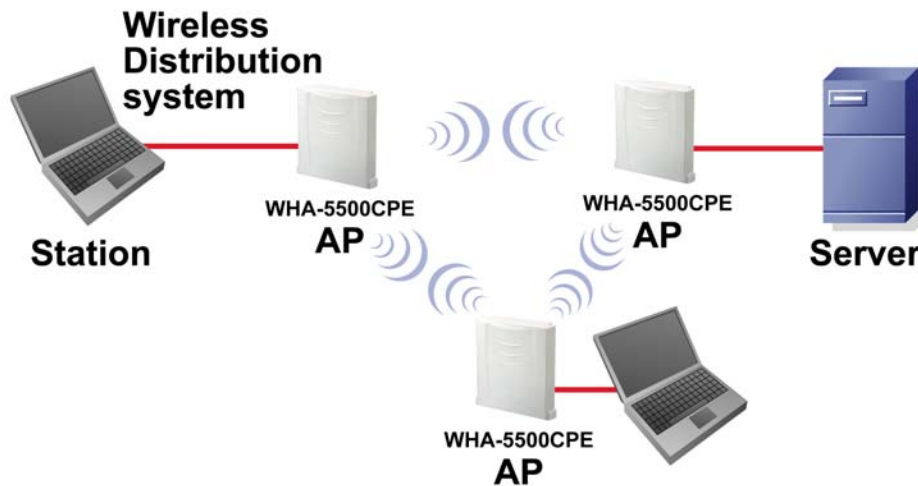
In Repeater mode, the WHA-5500CPE set as a repeater extends the range of wireless LAN.



1.3.3 WDS Bridge Mode

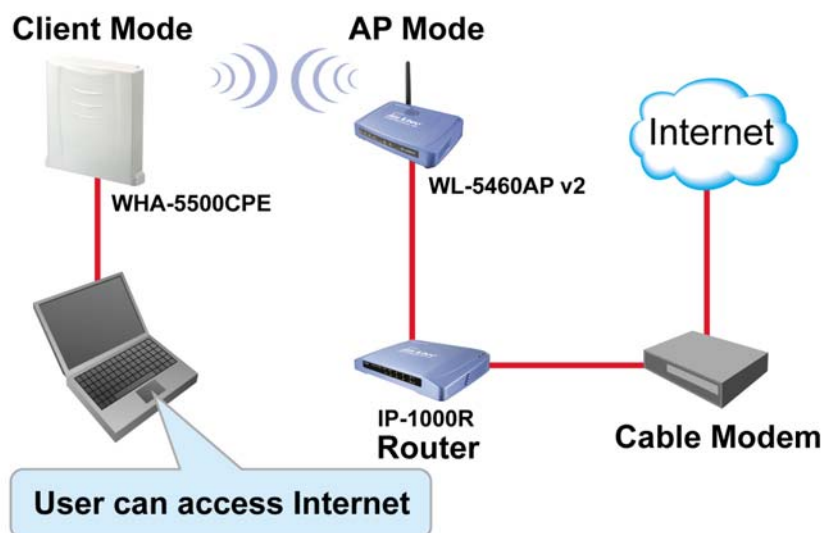
When configured to operate in the Wireless Distribution System (WDS) Mode, the WHA-5500CPE provides bridging functions between the LAN behind it and separates LANs behind other APs' operating in the WDS mode. The system will support up to **eight** APs in a WDS configuration.

Note that a WHA-5500CPE runs in the WDS mode can also support wireless stations simultaneously. See the diagram below:



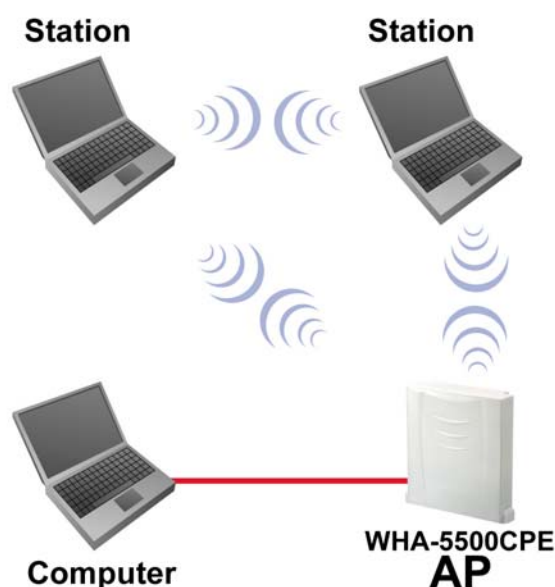
1.3.4 Client Infrastructure Mode

In Client Infrastructure mode, the WHA-5500CPE is connected to a computer and acts like a wireless station, so that the computer can wirelessly access the other network's services, such as Internet.



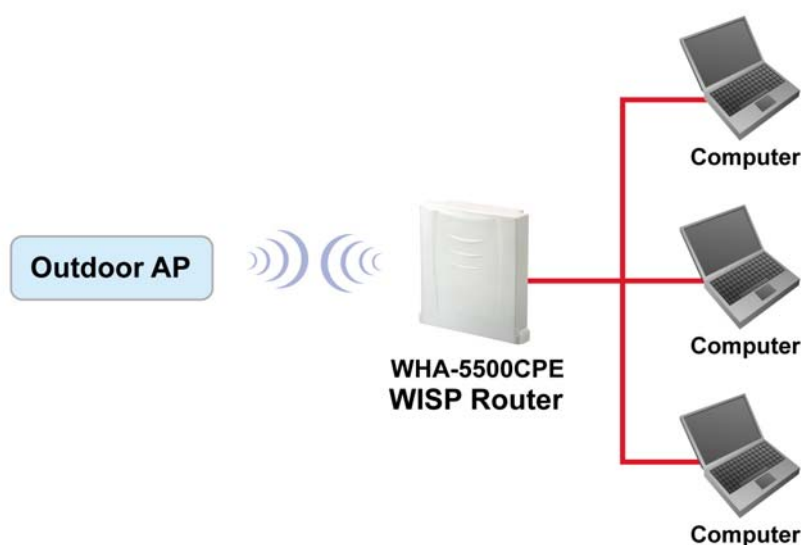
1.3.5 Client Ad Hoc Mode

In Client Ad Hoc mode, WHA-5500CPE is connected to a computer and acts like a wireless station, so that the computer can wirelessly share files and printers with other wireless stations.



1.3.6 WISP Router Mode

In WISP Router Mode, WHA-5500CPE is connected to several computers and acts like a Client mode AP. With IP sharing function, the computers can share the WISP connection via WHA-5500CPE.



1.4 Set up the device

The WHA-5500CPE can be managed remotely by a PC through either the wired or wireless network. To do this, the WHA-5500CPE must first be assigned an IP address, which can be done using one of the following two methods.

1.4.1 STATIC IP

The default IP address of the LAN interface of an WHA-5500CPE is a *private IP address* of **192.168.1.1**, and a *network mask* of 255.255.255.0. This means IP addresses of other devices on the LAN should be in the range of 192.168.1.2 to 192.168.1.254.

This IP address can be modified to either a different address in this same subnet or to an

address in a different subnet, depending on the existing network settings (if there is any) or user's preferences.

1.4.2 AUTOMATIC IP

The WHA-5500CPE can also be configured to “obtain” an IP address automatically from a DHCP server on the network. This address is called “dynamic” because it is only *dynamically* assigned to the device, which may change depends on the IP assignment policy used by the DHCP server on the network. Since the IP address in this case may change from time to time, this method is not recommended - unless the user uses UPnP or other management tools that do not depend on a fixed IP address.

2

Install the 802.11A Access Point

This section describes the installation procedure for the WHA-5500CPE. It starts with a summary of the content of the package you have purchased, followed by steps of how to power up and connect the WHA-5500CPE. Finally, this section explains how to configure a Windows PC to communicate with the WHA-5500CPE.

2.1 What's in the box?

The WHA-5500CPE package contains the following items:

- One WHA-5500CPE main unit
- One 48V 0.4A DC power adapter with a splitter
- Wall Mounting kit
- One CD of the WHA-5500CPE Quick Star Guide



WHA-5500CPE



Mounting Kits



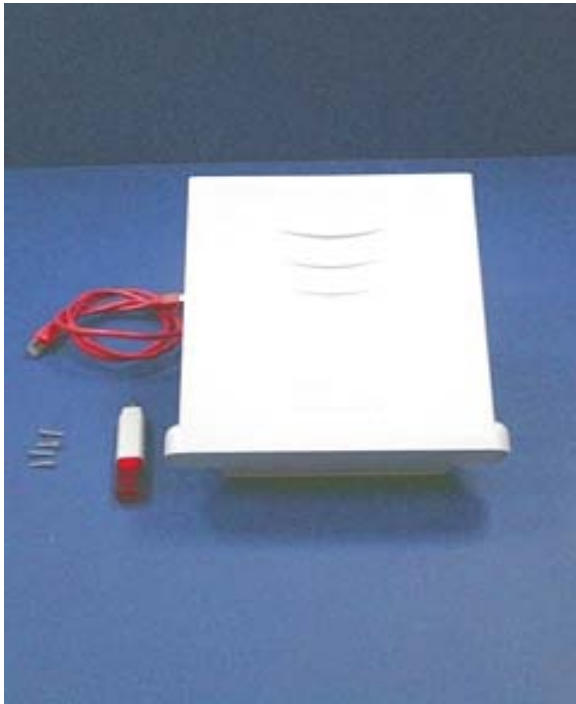
PoE Kits

Regarding to the specification of each application, the PoE Ethernet cable is not included in the package.

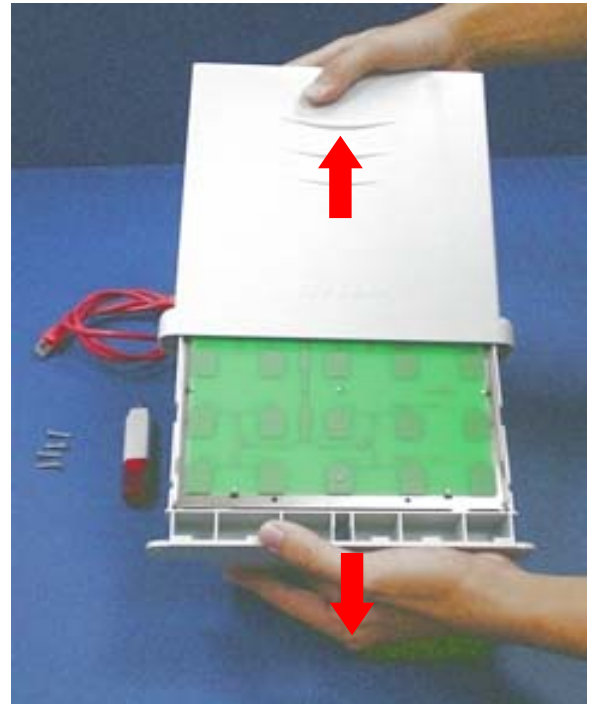
You may choose outdoor specification Ethernet cable according to the length you need.

2.2 Hardware Installation

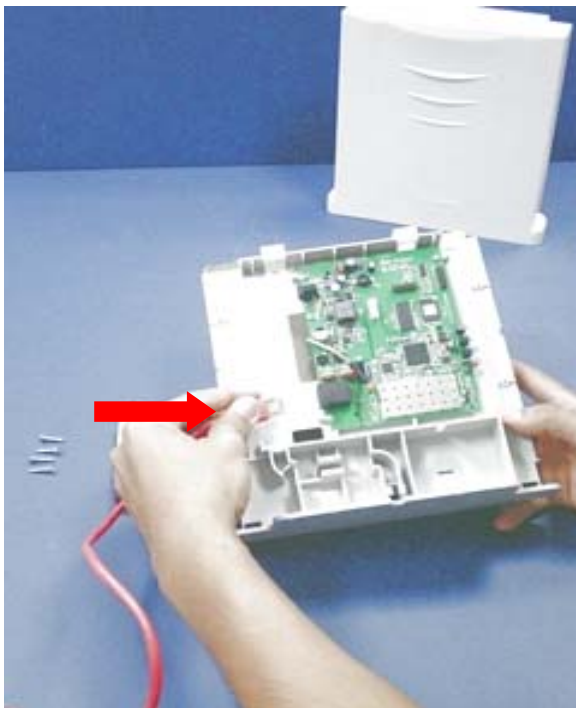
Please take the device unit from the color box, a scroll driver, an Ethernet cable with adequate length according to your application.



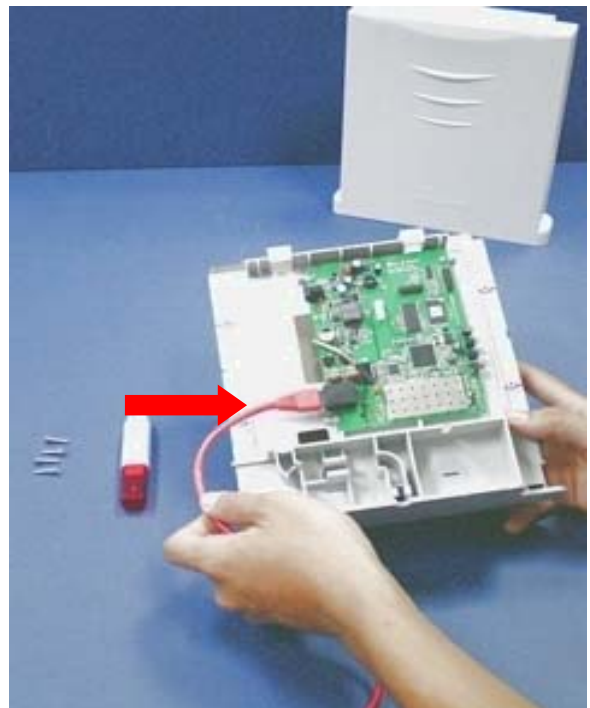
Step 1: A scroll driver and Ethernet Cable, four screws and WHA-5500CPE main unit



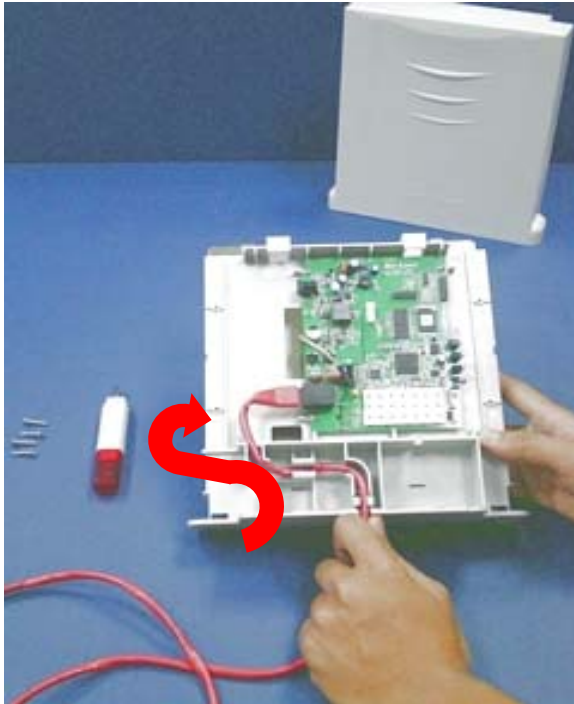
Step 2: Open the housing of WHA-5500CPE



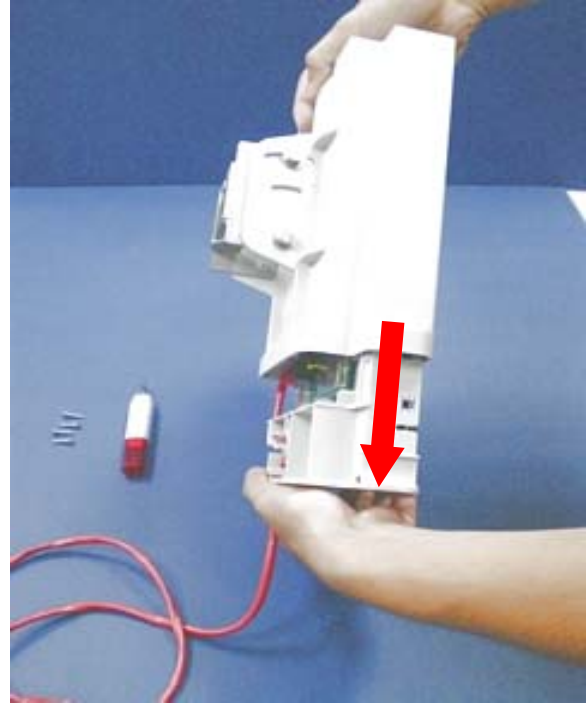
Step 3: Turn the WHA-5500CPE to another side, the RJ-45 jack is at the middle of LEFT side of main board.



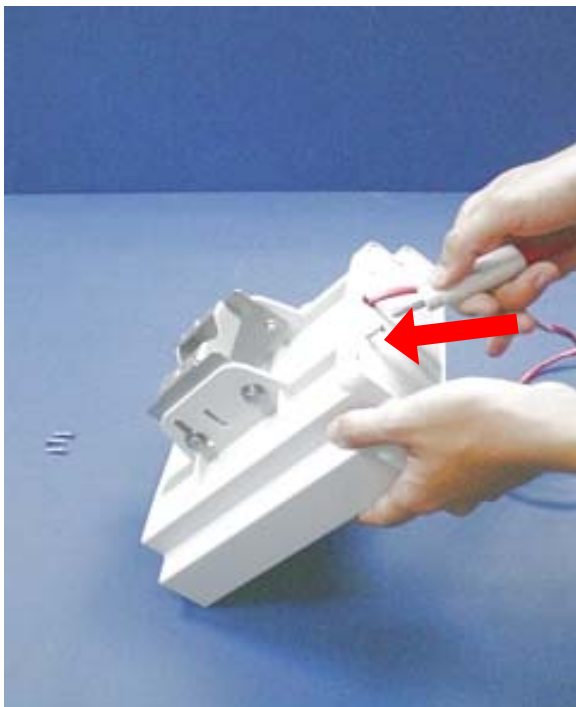
Step 4: Plug one side of RJ-45 cable into the Ethernet port.



Step 5: Put the Ethernet cable along the module, till the exit (at the bottom of Housing).



Step 6: Make sure that the other side of Ethernet cable is out of housing. Close the housing.

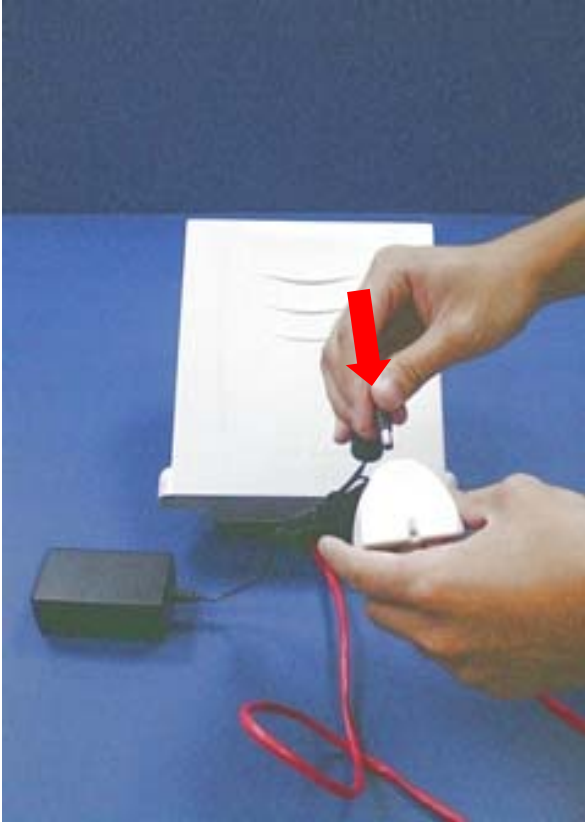


Step 7: Scroll up 4 screws well. Be careful, this is very important; it could protect your device against the water.

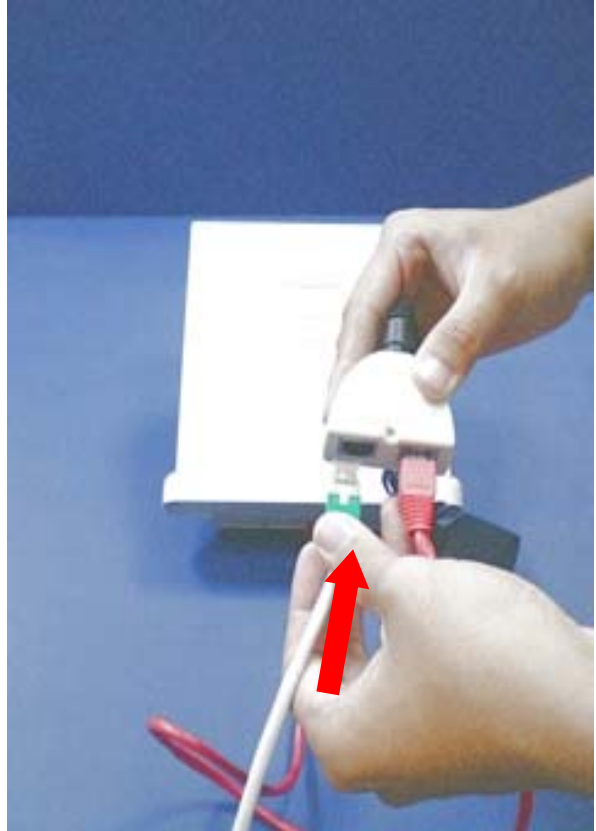


Step 8: Plug the Ethernet to the PoE "P + DATA OUT" jack of injector.

2. Install the WHA-5500CPE



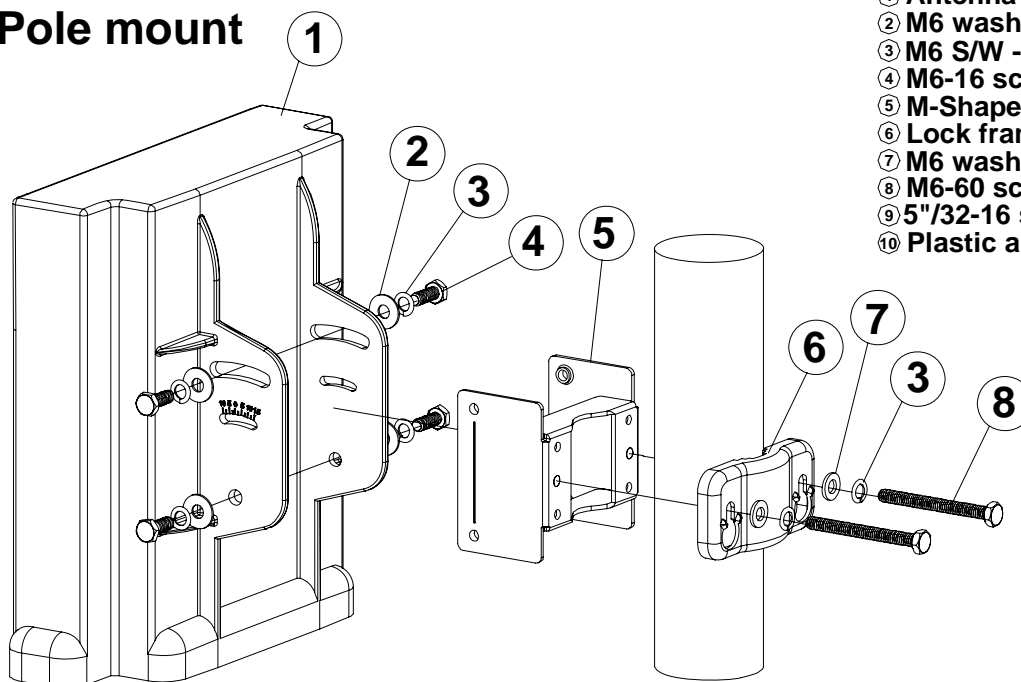
Step 9: Plug the power cord of adaptor into the injector “POWER IN” port.



Step 10: Plug the Data Ethernet cable to the port “DATA IN” of injector.

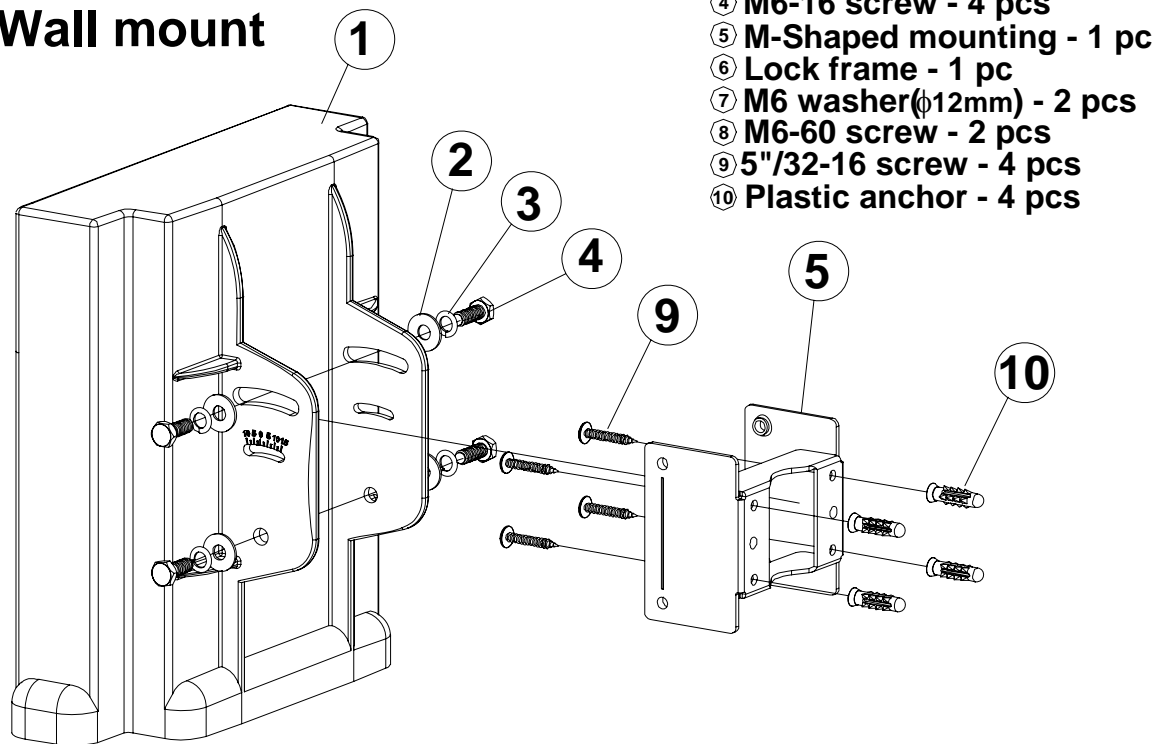
2.2.1 Mounting Configuration

Pole mount

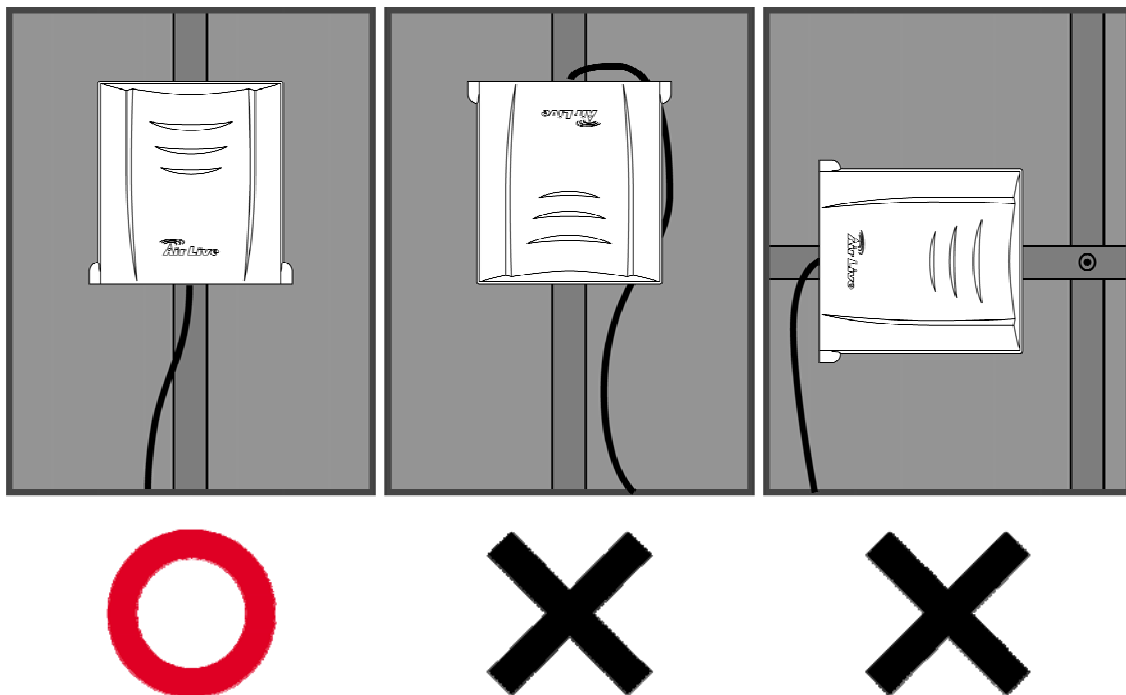


- ① Antenna body - 1pc
- ② M6 washer(ϕ 16mm) - 4 pcs
- ③ M6 S/W - 6 pcs
- ④ M6-16 screw - 4 pcs
- ⑤ M-Shaped mounting - 1 pc
- ⑥ Lock frame - 1 pc
- ⑦ M6 washer(ϕ 12mm) - 2 pcs
- ⑧ M6-60 screw - 2 pcs
- ⑨ 5"/32-16 screw - 4 pcs
- ⑩ Plastic anchor - 4 pcs

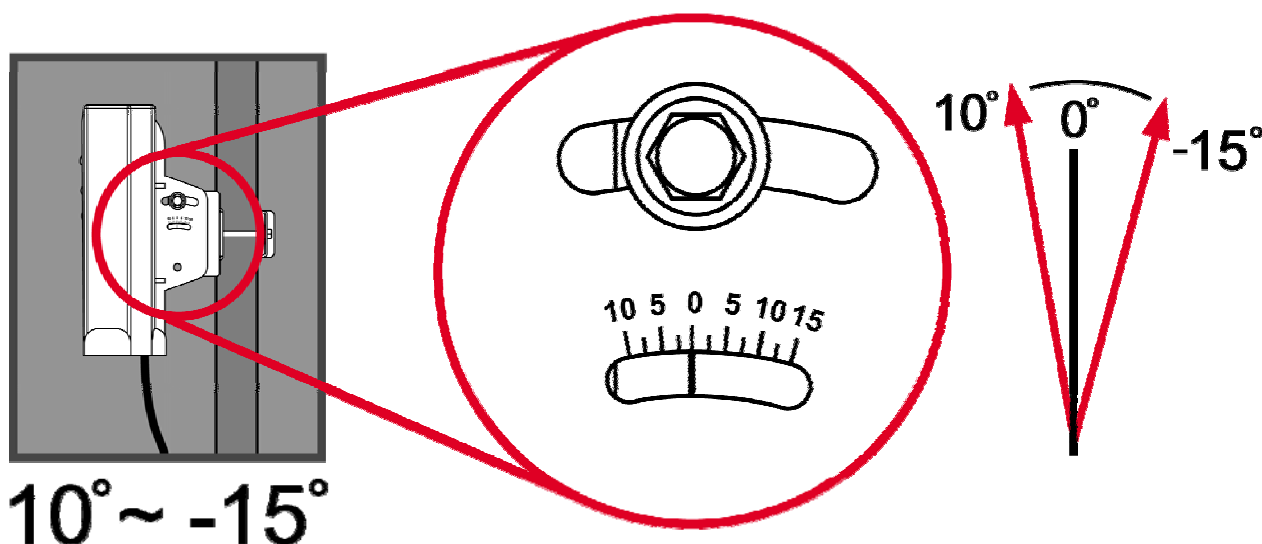
Wall mount



2.2.2 Antenna polarization



- Please install the CPE in the UP RIGHT position only.
- Do not put the CPE into water.



- Please do not tilt the CPE more than 15 degree angle from vertical.

2.3 Configuration steps

This section describes configuration required for the WHA-5500CPE before it can work properly in your network.

First, it is assumed that in your LAN environment, a separate DHCP server will be available for assigning dynamic (and often private) IP addresses to requesting DHCP clients.

Additionally, since you need to perform various configuration changes to the WHA-5500CPE, including the SSID, Channel number, the WEP key, ..., etc., it is necessary to associate a fixed IP address with the WHA-5500CPE, which is why the WHA-5500CPE will be shipped with a factory default private IP address of **192.168.1.1** (and a network mask of 255.255.255.0).

Therefore, during the system installation time, you need to build an isolated environment with the WHA-5500CPE and a PC, and then perform the following steps:

Step 1. Manually change the IP address of the PC to become 192.168.1.3.

Step 2. Connect the PC to the WHA-5500CPE *via* PoE and change its configuration to a static IP address based on your network environment. For example, if there is a DHCP server that assigns IP addresses from the range 192.168.23.10 - 192.168.23.254 to DHCP client devices, it can reserve 192.168.23.10 for the WHA-5500CPE and then the address pool with the DHCP server becomes 192.168.23.11 – 192.168.23.254.

If there is no DHCP server on your network environment, you just have to make sure that there is no machine in the environment has the same IP address as another machine.

Please note that after you change the IP address of the ACCESS POINT, the PC client may not be able to reach the ACCESS POINT. This is because they may no longer belong to the same IP network address space.

Step 3. Change the setting of the PC back to “obtain IP addresses dynamically”.

Now you can put the WHA-5500CPE and the PC to your network where the DHCP server is connected. From then on, any wireless client configured to “obtain IP

addresses dynamically” will work with the AP, with each other, and with devices on the wired LAN network.

2.4 Set up a wireless client as a DHCP client

The following will give detailed steps of how to configure a PC or a wireless client to “obtain IP addresses automatically”.

In the case of using a LAN attached PC, the PC must have an Ethernet interface installed properly, be connected to the WHA-5500CPE either directly or through an external LAN switch, and have TCP/IP installed and configured to obtain an IP address automatically from a DHCP server in the network.

In the case of using a wireless client, the client must also have an 802.11a wireless interface installed properly, be physically within the radio range of the WHA-5500CPE, and have TCP/IP installed and configured to obtain an IP address automatically from a DHCP server in the network.

Then perform the following steps for either of the cases above. To configure types of workstations other than Windows 95/98/NT/2000, please consult the manufacturer’s documentation.

- Step 1. From the Win95/98/2000 Start Button, select Settings, then Control Panel. The Win95/98/2000 Control Panel displays.
- Step 2. Double-click on the *Network* icon.
- Step 3. Check your list of Network Components in the Network window Configuration tab. If TCP/IP has already been installed, go to Step 8. Otherwise, select Add to install it now.
- Step 4. In the new Network Component Type window, select Protocol. In the new Select Network Protocol window, select Microsoft in the Manufacturers area.
- Step 5. In the Network Protocols area of the same window, select TCP/IP, then click OK. You may need your Win95/98 CD to complete the installation. After TCP/IP installation is complete, go back to the Network window described in Step 4.
- Step 6. Select TCP/IP in the list of Network Components.
- Step 7. Click **Properties**, and check the settings in each of the TCP/IP Properties window: **Bindings Tab**: both **Client for Microsoft Networks** and **File and printer sharing for Microsoft Networks** should be selected. **Gateway Tab**: All fields should be blank. **DNS Configuration Tab**: **Disable DNS** should be selected. **IP Address Tab**: **Obtain IP address automatically** should be selected.
- Step 8. With the WHA-5500CPE powered on, reboot the PC/wireless client. After the PC/wireless client is re-booted, you should be ready to configure the WHA-5500CPE. See Chapter 3.

The procedure required to set a static IP address is not too much different from the procedure required to set to “obtain IP addresses dynamically” - except that at the end of step 7, instead of selecting “obtain IP addresses dynamically, you should specify the IP address explicitly.

3

Basic Configuration

This section describes the basic configuration procedure for the WHA-5500CPE. It describes how to set up the WHA-5500CPE for wireless connections, and the configuration of the local LAN environment. All basic configurations may be effected through a standard Web browser such as Microsoft Internet Explorer. From a PC that has been configured as described in Chapter 2, enter the IP address of the WHA-5500CPE as the URL in your browser, e.g. <http://192.168.1.1>.



The IP address of your PC must be in the same IP subnet as the WHA-5500CPE.

The Home Page of the WHA-5500CPE screen will appear. Its main menu displays on the right hand side of the window. The main menu includes the following choices: Setup Wizard, Device Status, Advanced Settings, System Tools, and Help.

Log On

If you attempt to access a configuration item from the browser menu, an administrator logon screen, shown below, will appear.



AirLive® Multi-Function AP
802.11a/b/g www.airlive.com

Please enter your password:

***** **LOG ON**

(Forgot your password? - see the User Guide for instructions.)

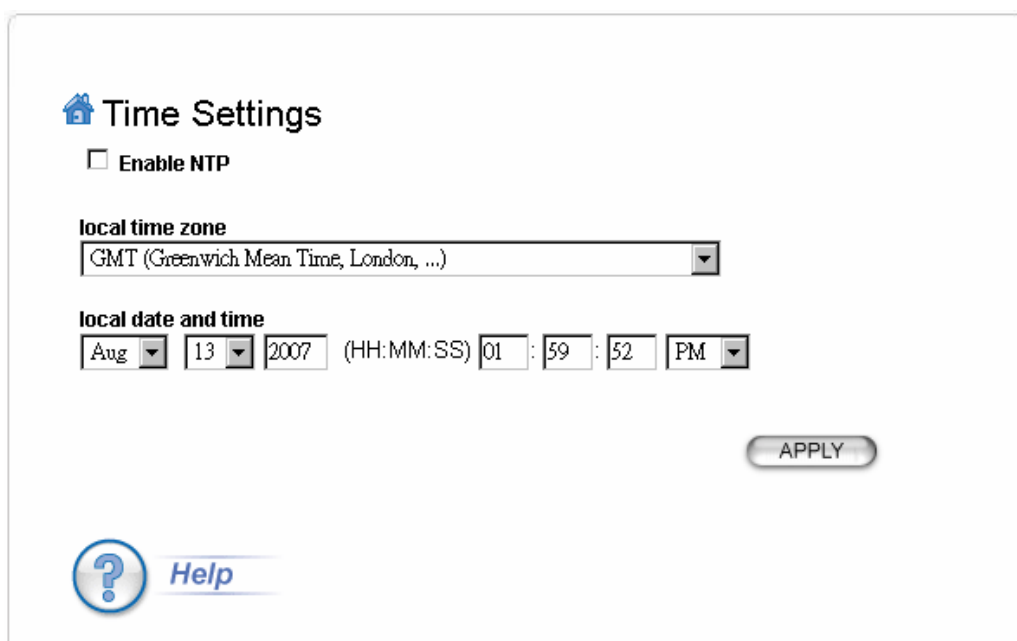
If you are logging on for the first time, you should use the factory default setting “**airlive**”. The password is always displayed as a string of wildcards or dots. Click the **LOG ON** button to start the configuration session.

3.1 Setup wizard

The Setup Wizard will guide you through a series of configuration screens to set up the basic functionality of the device. Every time you modify the settings, remember to click **APPLY** button to save the changes.

3.1.1 TIME SETTINGS

[Setup Wizard>>Time Settings](#)




Time Settings

☐ Enable NTP

local time zone
 GMT (Greenwich Mean Time, London, ...) ▼

local date and time
 Aug ▼ 13 ▼ 2007 (HH:MM:SS) 01 : 59 : 52 PM ▼

APPLY

 [Help](#)

After logging on, the **Time Settings** page appears. The device time is automatically set to the local time of the management PC at the first time a connection is made. To modify the device’s time, modify the appropriate fields, then click **APPLY**.

3.1.2 DEVICE IP SETTINGS

[Setup Wizard>> Device IP Settings](#)

Device IP Settings

You can select one of the following two approaches to assign an IP address to this device.

☒ **Assign static IP to this device.**

IP Address:	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
IP Subnet Mask:	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
Gateway IP Address:	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>	<input type="text" value="254"/>
DNS Server :	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

☐ **Use the DHCP client protocol to automatically get the IP address for this device.**

Selecting this option will disable your DHCP server automatically.

APPLY

NOTE: Changes to this page will not take effect until you click FINISH on the save config page.



The **Device IP Settings** screen allows you to configure the IP address and subnet of the device. Although you can rely on a DHCP server to assign an IP address to the WHA-5500CPE automatically, it is recommended that you configure a static IP address manually in most applications.

If you choose to assign the IP address manually, enable the checkbox of “Assign static IP to this device” and then fill in the following fields

IP Address and **IP Subnet Mask:** Default values are 192.168.1.1 and 255.255.255.0 respectively. It is important to note that there are similar addresses falling in the standard private IP address range and it is an essential security feature of the device. Because of this private IP address, the device can no longer be accessed (seen) from the Internet.

Gateway IP Address: Enter the IP address of your default gateway.

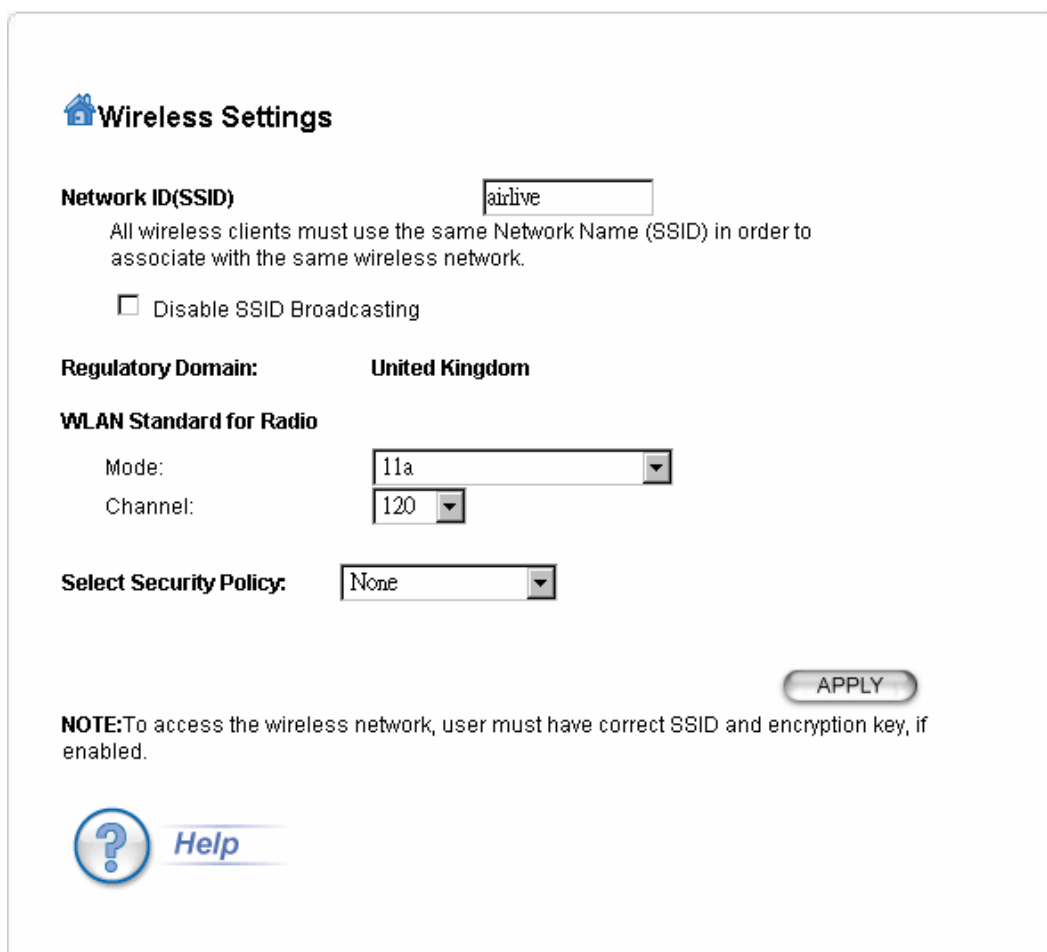
DNS Server: The Domain Name System (DNS) is a server on the Internet that translates logical names such as “www.yahoo.com” to IP addresses like 66.218.71.80. In order to do this, a query is made by the requesting device to a DNS server to provide the necessary information. If your system administrator requires you to manually enter the DNS Server addresses, you should enter them here.

Click **APPLY** to go to the next screen.

If you choose to use a DHCP Server to acquire an IP address for the WHA-5500CPE automatically, enable the checkbox that says, “Use the DHCP client protocol to automatically get the IP address for this device”. Then click Next to go to the next screen. Again, as a reminder, it is recommended that your WHA-5500CPE should be assigned a static IP address in order to make it easy for you to manage the device later on.

3.1.3 WIRELESS SETTINGS

Setup Wizard>>Wireless Settings



Wireless Settings

Network ID(SSID)
 All wireless clients must use the same Network Name (SSID) in order to associate with the same wireless network.

☐ Disable SSID Broadcasting

Regulatory Domain: **United Kingdom**


WLAN Standard for Radio

Mode:
 Channel:

Select Security Policy:

APPLY

NOTE: To access the wireless network, user must have correct SSID and encryption key, if enabled.

 [Help](#)

Network ID (SSID): The SSID is the network name used to identify a wireless network. The SSID must be the same for all devices in the wireless network (i.e. in the same BSS). Several access points on a network can have the same SSID. The SSID length is up to 32 characters. The default SSID is “**airlive**”.

Disable SSID Broadcasting: An access point periodically broadcasts its SSID along with other information, which allows client stations to learn its existence while searching for access points in a wireless network. Check **Disable SSID Broadcasting** if you do not want the device to broadcast the SSID.

Regulatory Domain: Please make sure that your regulatory domain matches your region. The default value is “**United Kingdom**”.

WLAN Mode: Select “**11a**” or “**Super A**”. Choosing “**11a**” allows only 802.11a client stations to get associated. 802.11a outdoor range spectrum AP with maximum data rate 54Mbps; **Super A** mode is Atheros proprietary data exchange standard, it allows AP/Client to connect with other AirLive product of which Atheros Super A mode is available.

Channel: Select a channel from the drop down menu. All devices in a BSS must use the same channel. You can select **Auto** to let the system pick up the best channel for you.



The available channels are different from country to country and for different WLAN mode.

Security Policy: You can select different security policy to provide association authentication and/or data encryption.

WEP

[Setup Wizard>>Wireless Settings >>Select Security Policy>>WEP](#)

Select Security Policy:

WEP

Encryption

Enabling encryption will secure data and prevent unauthorized users from accessing your wireless network. Identical encryption keys must be entered on all authorized wireless clients.

Authentication type

☒ AUTO


Select one of the WEP keys for the wireless network:

Encrypt data transmitting with WEP Key 1

WEP Key 1	WEP64-ASCII	
WEP Key 2	WEP64-ASCII	
WEP Key 3	WEP64-ASCII	
WEP Key 4	WEP64-ASCII	

APPLY

NOTE:To access the wireless network, user must have correct SSID and encryption key, if enabled.


[Help](#)

WEP allows you to use data encryption to secure your data from being eavesdropped by malicious people. It allows 3 types of key: 64 (**WEP64**), 128 (**WEP128**), and 152 (**WEP152**) bits. You can configure up to 4 keys using either **ASCII** or **Hexadecimal** format.

Key Settings: The length of a **WEP64** key must be equal to 5 bytes, a **WEP128** key is 13 bytes, and a **WEP152** key is 16 bytes.

Key Index: You have to specify which of the four keys will be active.

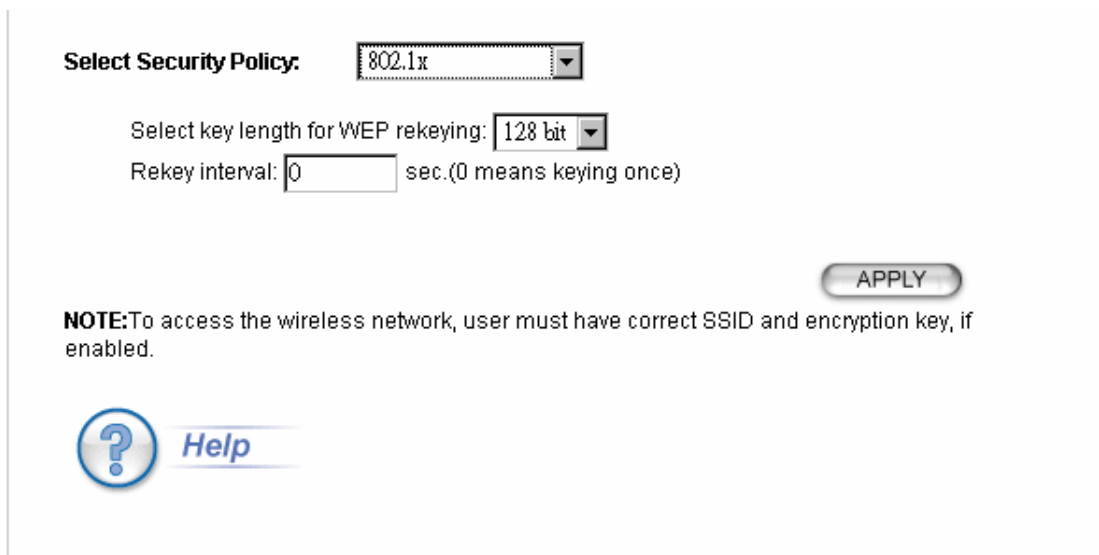
Once you enable the WEP function, please make sure that both the WHA-5500CPE and the wireless client stations use the same key.



Some wireless client cards only allow Hexadecimal digits for WEP keys. Please note that when configuring WEP keys, a WEP128 ASCII key looks like “**This is a key**”(13 characters), while a WEP128 Hex key looks like “**546869732069732061206b6579**”(26 HEX) (hexadecimal notation are 0-9 and A-F).

802.1x

[Setup Wizard>>Wireless Settings >>Select Security Policy>>802.1x](#)




Select Security Policy: 802.1x

Select key length for WEP rekeying: 128 bit

Rekey interval: 0 sec.(0 means keying once)

APPLY

NOTE: To access the wireless network, user must have correct SSID and encryption key, if enabled.

 [Help](#)

802.1x allows users to leverage a RADIUS server to do association authentications. You can also enable dynamic WEP key (128 bit) to have data encryption. Here you do not have to enter the WEP key manually because it will be generated automatically and dynamically.

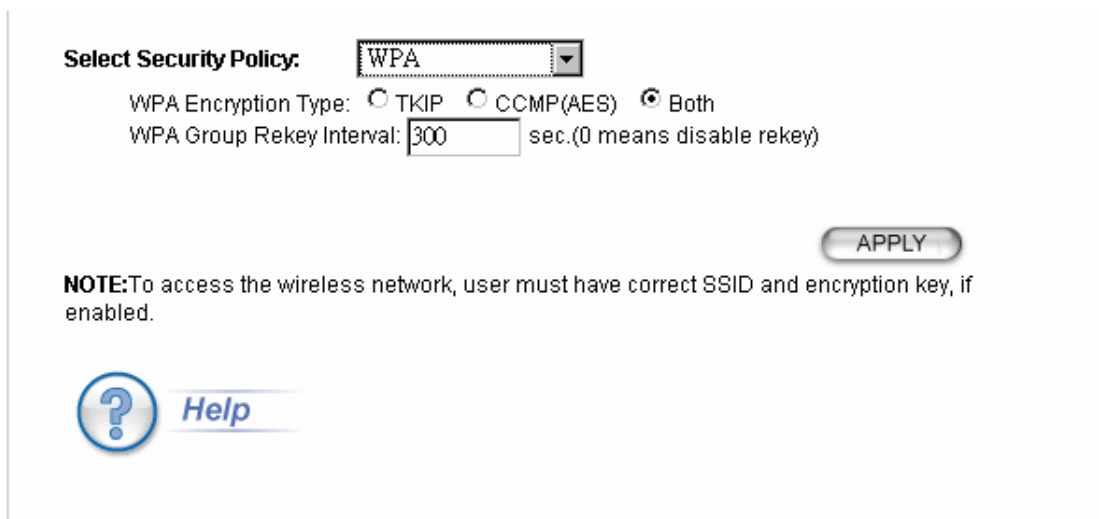
Rekey interval is time period that the system will change the key periodically. The shorter the interval is, the better the security is.



After you have finished the configuration wizard, you have to configure the RADIUS Settings in Advanced Settings in order to make the 802.1x function work.

WPA

[Setup Wizard](#)>>[Wireless Settings](#) >>[Select Security Policy](#)>>WPA




Select Security Policy: WPA

WPA Encryption Type: ☐ TKIP ☐ CCMP(AES) ☒ Both

WPA Group Rekey Interval: 300 sec.(0 means disable rekey)

APPLY

NOTE: To access the wireless network, user must have correct SSID and encryption key, if enabled.

 [Help](#)

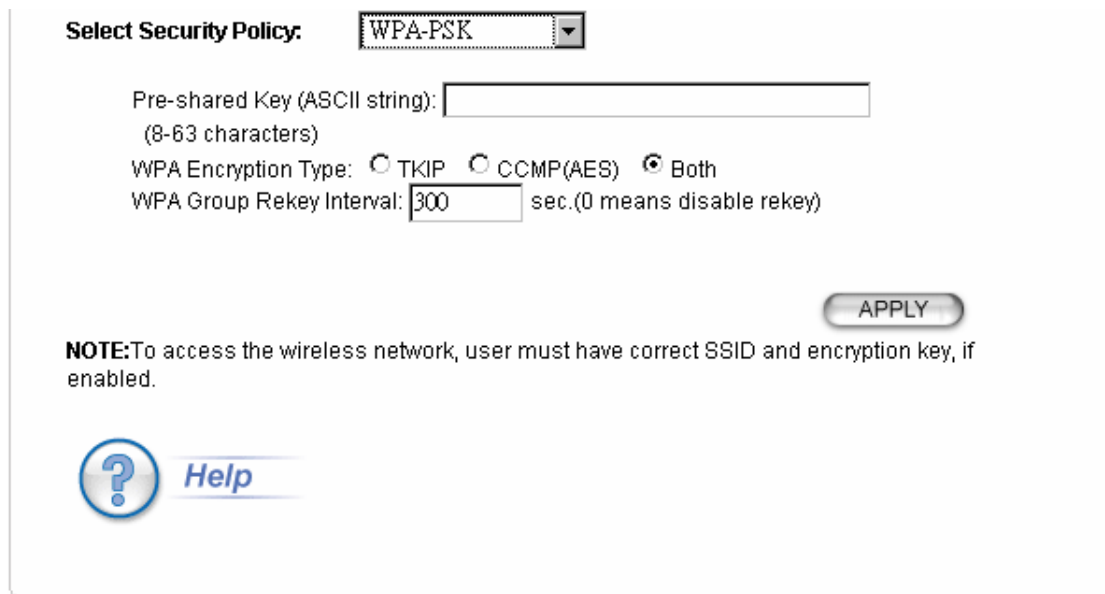
Wi-Fi Protected Access (WPA) requires a RADIUS server available in order to do authentication (same as 802.1x), thus there is no shared key required.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-PSK

Setup Wizard>>Wireless Settings >>Select Security Policy>>WPA-PSK



The image shows a web-based configuration interface for WPA-PSK. At the top, there is a label 'Select Security Policy:' followed by a dropdown menu showing 'WPA-PSK'. Below this, there is a text input field for the 'Pre-shared Key (ASCII string):' with a note '(8-63 characters)' underneath. To the right of the key field are three radio buttons for 'WPA Encryption Type': 'TKIP', 'CCMP(AES)', and 'Both', with 'Both' being selected. Below the encryption type is a text input field for 'WPA Group Rekey Interval:' with the value '300' and a note 'sec.(0 means disable rekey)'. On the right side of the form is an 'APPLY' button. At the bottom left, there is a 'NOTE:' stating 'To access the wireless network, user must have correct SSID and encryption key, if enabled.' and a 'Help' link with a question mark icon.

Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) provides better security than WEP keys. It does not require a RADIUS server in order to provide association authentication, but you do have to enter a shared key for the authentication purpose. The encryption key is generated automatically and dynamically.

Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WHA-5500CPE and the wireless client stations use the same key.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA2

[Setup Wizard>>Wireless Settings >>Select Security Policy>>WPA2](#)

Select Security Policy: WPA2

WPA2 Encryption Type: ☐ TKIP ☐ CCMP(AES) ☒ Both

WPA2 Group Rekey Interval: sec.(0 means disable rekey)

APPLY

NOTE: To access the wireless network, user must have correct SSID and encryption key, if enabled.

[Help](#)

WPA2 stands for Wi-Fi Protected Access 2. It provides stronger data protection and network access control than WPA. Only authorized users can access the wireless networks.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA2-PSK

[Setup Wizard>>Wireless Settings >>Select Security Policy>>WPA2-PSK](#)

Select Security Policy: WPA2-PSK

Pre-shared Key (ASCII string):
(8-63 characters)

WPA Encryption Type: ☐ TKIP ☐ CCMP(AES) ☒ Both

WPA2 Group Rekey Interval: sec.(0 means disable rekey)

APPLY

NOTE: To access the wireless network, user must have correct SSID and encryption key, if enabled.

[Help](#)

Enter the Pre-shared Key to initiate WPA security. All devices try to access the network should have the matching encryption key.

Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WHA-5500CPE and the wireless client stations use the same key.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-AUTO

[Setup Wizard>>Wireless Settings >>Select Security Policy>>WPA-AUTO](#)

Select Security Policy: WPA-AUTO

WPA-AUTO Encryption Type: ☐ TKIP ☐ CCMP(AES) ☒ Both

WPA-AUTO Group Rekey Interval: sec.(0 means disable rekey)

APPLY

NOTE:To access the wireless network, user must have correct SSID and encryption key, if enabled.

[Help](#)

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-PSK-AUTO

[Setup Wizard>>Wireless Settings >>Select Security Policy>>WPA-PSK-AUTO](#)

Select Security Policy: WPA-PSK-AUTO

Pre-shared Key (ASCII string):
(8-63 characters)

WPA-AUTO Encryption Type: ☐ TKIP ☐ CCMP(AES) ☒ Both

WPA-AUTO Group Rekey Interval: sec.(0 means disable rekey)

APPLY

NOTE:To access the wireless network, user must have correct SSID and encryption key, if enabled.

[Help](#)

WPA-PSK-AUTO tries to authenticate wireless clients using WPA-PSK or WPA2-PSK.

Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WHA-5500CPE and the wireless client stations use the same key.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

3.1.4 FINISH SETUP WIZARD AND SAVE YOUR SETTINGS

After stepping through the Wizard's pages, you can click the **APPLY** button for your modification to take effect. This also makes your new settings saved into the permanent memory on your system.

Congratulations! You are now ready to use the WHA-5500CPE.



If you change the device's IP address, as soon as you click on FINISH you will no longer be able to communicate with your WHA-5500CPE. You need to change your IP address and then re-boot your computer in order to resume the communication.


3.2 Advanced settings

The advanced settings tab on the top row of the window allows you to perform modifications that normally you may not need to do for general operations except changing your password from the default factory setting (this is highly recommended for security purposes).

3.2.1 PASSWORD SETTINGS

[Advanced Settings](#)>> [Password Settings](#)

The default factory password is “**password**”. To change the password, press the **Password Settings** button to enter the **Password Settings** screen; then enter the Current Password followed by the New Password twice. The entered characters will appear as asterisks.


 **Password Settings**
Change Password


To change your administrative password, enter your current password and then the new password twice.

Current Password:

New Password:

Re-enter New Password:



 [Help](#)

3.2.2 SYSTEM MANAGEMENT

[Advanced Settings>> System Management](#)

Clicking the **System Management** button to configure system related parameters to for the WHA-5500CPE.

System Management

System Administration
 HTTP Port No.: timeout: minutes

UPnP
☒ Enable UPnP

Bridge
☐ Enable STP

Syslog
☐ Enable Syslog
 Syslog server IP address: . . .

APPLY

NOTE: Syslog is a standard for logging system events (IETF RFC-3164). System event messages generated by the wireless access point will be sent to a Syslog daemon running on a server identified by this IP address.

[Help](#)

HTTP Port No.: HTTP stands for Hyper Text Transfer Protocol. The default port for the HTTP Web server is 80.

Time-out: This setting specifies the duration of idle time (inactivity) before a web browser or telnet management session times out. The default is 10 minutes.

UPnP: The Universal Plug and Play (UPnP) feature allows a Windows XP/ME PC to discover this WHA-5500CPE and automatically show an icon on the screen. Then a user can double-click the icon to access this device directly (without having to find out its IP address).


Syslog: Syslog is an IETF (Internet Engineering Task Force - the Internet standards body)-conformant standard for logging system events (RFC-3164). When the WHA-5500CPE encounters an error or warning condition (e.g., a log-in attempt with an invalid password), it will create a log in the system log table. To be able to remotely view such system log events, you need to check the **Enable Syslog** box and configure the IP address of a Syslog daemon. When doing so, the WHA-5500CPE will send logged events over network to the daemon for future reviewing.

Syslog server IP address: System event messages generated by the wireless access point will be sent to a Syslog daemon running on a server identified by this IP address.

3.2.3 SNMP Settings

[Advanced Settings>>SNMP Settings](#)

This screen allows you to configure SNMP parameters including the system name, the location and contact information.


SNMP Settings

☒ **Enable SNMP**

Assign system information:

System Name:

System Location:

System Contact:

Assign the SNMP community string:

Community String For Read:

Community String For Write:

Assign a specific name and IP address for your SNMP trap manager:


Name:

IP Address: . . .

ADD

Select	Name	IP Address	Enable
-	-	-	-

DELETE SELECTED


[Help](#)

System Name: A name that you assign to your 802.11a+g Router. It is an alphanumeric string of up to 30 characters.

System Location: Enter a system location.

System Contact: Contact information for the system administrator responsible for managing your 802.11a+g Router. It is an alphanumeric string of up to 60 characters.

Community String For Read: If you intend the router to be managed from a remote SNMP management station, you need to configure a read-only “community string” for read-only operation. The community string is an alphanumeric string of up to 15 characters.

Community String For Write: For read-write operation, you need to configure a write “community string”.

Assign a specific name and IP address for your SNMP trap manager:

A trap manager is a remote SNMP management station where special SNMP trap messages are generated (by the router) and sent to in the network.

You can define trap managers in the system.

You can add a trap manager by entering a **name**, an **IP address**, followed by pressing the **ADD** button.

You can delete a trap manager by selecting the corresponding entry and press the **DELETE SELECTED** button.

To enable a trap manager, check the **Enable** box in the corresponding entry; to disable it, un-check the **Enable** box.

3.2.4 MAC FILTERING SETTINGS


[Advanced Settings>>Mac Filtering Settings](#)

The WHA-5500CPE allows you to define a list of MAC addresses that are allowed or denied to access the wireless network.

Disable MAC address control list: When selected, no MAC address filtering will be performed.

Enable GRANT address control list: When selected, data traffic from only the specified devices in the table will be allowed in the network.

Enable DENY address control list: When selected, data traffic from the devices specified in the table will be denied/discarded by the network.


MAC Filtering Settings

This feature allows you to define a list of MAC addresses that are authorized to access or denied from accessing the wireless network.

☒ **Disable MAC address control list**
 No MAC address filtering is performed.

☐ **Enable GRANT address control list**
 Allow data traffic from devices listed in the table to access the network.

☐ **Enable DENY address control list**
 Deny /discard data traffic from devices listed in the table.

APPLY

Mnemonic Name:


MAC Address: - - - - -

ADD

Select	Name	MAC Address
-	-	-

DELETE SELECTED

NOTE: Incorrect configuration may cause undesirable behavior. Please refer to the user manual for more details


[Help](#)

To add a MAC address into the table, enter a **Mnemonic Name** and the **MAC Address**, and then click **ADD**. The table lists all configured MAC Filter entries.

To delete entries, check the corresponding **Select** boxes and then press **DELETE SELECTED**.

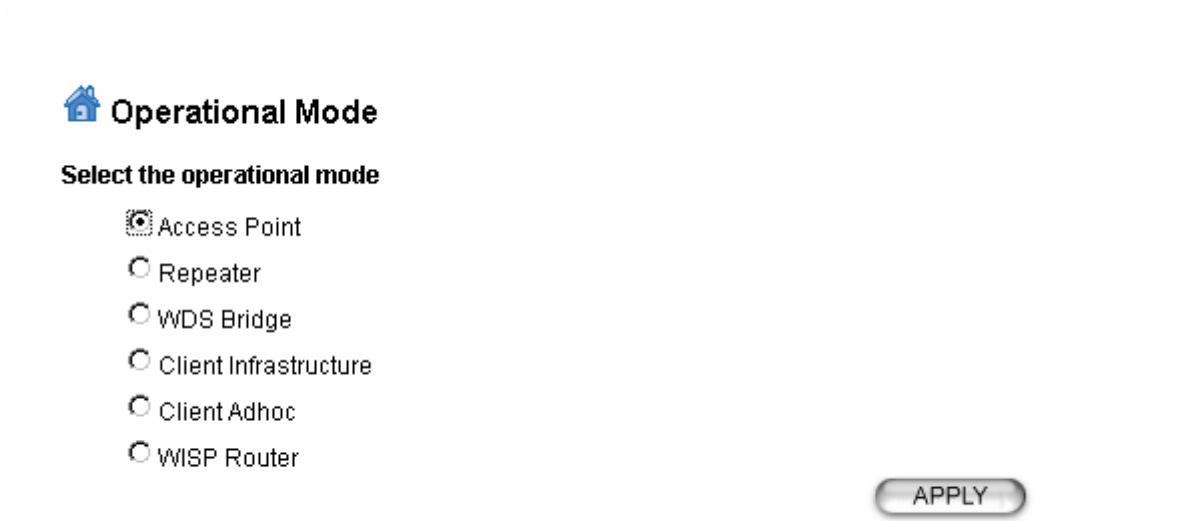
3.2.5 OPERATIONAL MODE


The WHA-5500CPE can be configured to operate in one of the following modes as mentioned previously in Chapter 1:

(1) Access Point (2) Repeater (3) WDS Bridge (4) Client Infrastructure
(5) Client Adhoc (6) WISP Router

3.3 Access Point Mode Settings

[Advanced Settings>> Operation Mode>> Access Point](#)



 **Operational Mode**

Select the operational mode

- ☒ Access Point
- ☐ Repeater
- ☐ WDS Bridge
- ☐ Client Infrastructure
- ☐ Client Adhoc
- ☐ WISP Router

APPLY

Select “Access Point” mode and then press **APPLY** button.

3.3.1 Wireless Settings

[Advanced Setting>> Wireless Settings](#)

Wireless Settings

Beacon Interval: msec. (range: 20-1000, default 100)
RTS Threshold: bytes (range: 0-2347, default 2347)
Fragmentation: bytes (range: 256-2346, default 2346)
DTIM Interval: (range 1-255, default 1)
User Limitation: (range: 1-100, default 100)
Age Out Timer: (min. range: 1-1000, default 5)
Transmit Power: (Reduce Tx Power between 0~14 dB)
Rate Control: Mbps
AckTimeOut (11a/SuperA): μ s (range: 10-255, default 25)

☐ Enable Radio eXtended Range
☐ Enable privacy separator
☐ Enable STP
☒ Enable 802.11d

ACK Calculator

DEFAULT

APPLY

Beacon Interval: The WHA-5500CPE broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

RTS Threshold: RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

DTIM Interval: The WHA-5500CPE buffers packets for stations that operate in the power-saving mode. The Delivery Traffic Indication Message (DTIM) informs such power-conserving stations that there are packets waiting to be received by them. The DTIM interval specifies how often the beacon frame should contain DTIMs. It should have a value between 1 to 255, with a default value of **3**.

User Limitation: The range of user limitation is from 1 to 100.

Age Out Timer: Set the age out time. The default is 300 sec.

Transmit Power: Transmit power output depends upon the size and RF characteristics because that will determine the number of APs, channels, and need for antennas.

Ack TimeOut (11a): The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to [Section 3.9](#).

Enable Radio eXtended Range: Select the check box to enable the Atheros's eXtended Range(XR) technology to extend the wireless coverage range.


Enable privacy separator: Select the check box to prohibit data transmission between client stations.

Enable WDS: Select the check box to enable WDS (Wireless Distribution System).

Enable 802.11d: Select the check box to enable 802.11d. 802.11d is a standard for use in countries where systems using other standards in the 802.11 family are not allowed to operate.

3.3.2 SSID Settings

[Advanced Settings >> SSID Settings](#)

 **SSID Settings**

☐ Enable VLAN for all SSIDs
☐ Enable DiffServ Marking

APPLY

SSID Name	VLAN ID/Priority	Security
<input type="radio"/> airlive	-	None

NEW

DELETE SELECTED

SSID Name:

☐ Disable SSID Broadcasting

Select Security Policy:

APPLY

SSID, a name for an access point (or a network), differentiates one WLAN from another. All devices in a same specific WLAN must use the same SSID.

VLAN: VLAN stands for Virtual Local Area Network. It is a technique allows one or more physical LAN routers or APs to deliver packets as if they were a single physical router or AP.


DiffServ Marking: Enable DiffServ Marking to have better traffic prioritization and bandwidth management.

Disable SSID Broadcasting: Select this check box to hide the SSID.

Security Policy: Select security policy. “None”, “WEP”, “802.1x”, “WPA”, “WPA-PSK”, “WPA2”, “WPA2-PSK”, “WPA-AUTO” or “WPA-PSK-AUTO”.

3.3.3 QoS Settings

[Advanced Settings >> QoS Settings](#)


QoS Settings


☒ **Enable WMM**

WMM Parameters of Access Point

AC TYPE	ECWMin	ECWMax	AIFS	TxopLimit-11b(μs)	TxopLimit-11g(μs)	ACMAck-policy
AC_BE(0)	4	6	3	0	0	<input type="checkbox"/> <input type="checkbox"/>
AC_BK(1)	4	10	7	0	0	<input type="checkbox"/> <input type="checkbox"/>
AC_VI(2)	3	4	1	6016	3008	<input type="checkbox"/> <input type="checkbox"/>
AC_VO(3)	2	3	1	3264	1504	<input type="checkbox"/> <input type="checkbox"/>

WMM Parameters of Station

AC TYPE	ECWMin	ECWMax	AIFS	TxopLimit-11b(μs)	TxopLimit-11g(μs)	ACM
AC_BE(0)	4	10	3	0	0	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	0	<input type="checkbox"/>
AC_VI(2)	3	4	2	6016	3008	<input type="checkbox"/>
AC_VO(3)	2	3	2	3264	1504	<input type="checkbox"/>


[Help](#)

QoS stands for Quality of Service which attempts to provide different levels of quality to different types of network traffic.

WMM stands for Wi-Fi Multimedia. WMM defines quality of service (QoS) in wireless networks. WMM improves audio, video and voice applications transmitted over wireless networks. WMM adds prioritized capabilities to wireless networks and optimizes the performance when multiple concurring applications.

To **Enable WMM**, WMM Parameters of Access Point and Station are indicated. The following information is listed: AC TYPE (AC_BE; Best Effort) (AC_BK; Background)(AC_VI; Video)(AC_VO;Voice)/ ECWMin/ ECWMax/ AIFS/ TxopLimit (11b)/ TxopLimit (11g)ACM

and Ack-policy.

3.3.4 RADIUS Settings

[Advanced Settings >> RADIUS Setting](#)

RADIUS Settings

RADIUS Server

☐ Enable RADIUS Server

Server IP: 0 . 0 . 0 . 0

Port Number: 1812

RADIUS Type: RADIUS

Shared Secret:

Secondary RADIUS Server

☐ Enable RADIUS Server

Server IP: 0 . 0 . 0 . 0

Port Number: 1812

RADIUS Type: RADIUS

Shared Secret:

RADIUS Server Reattempt Period 60 **Seconds**

APPLY

[Help](#)

RADIUS servers provide centralized authentication services to wireless clients. Two RADIUS servers can be defined: one acts as a primary, and the other acts as a backup.

MAC address filtering based authentication requires a MAC address filter table to be created in either the WHA-5500CPE (as described in Chapter 3.2.3 MAC Filtering Settings) and/or the RADIUS server. During the authentication phase of a wireless station, the MAC address filter table is searched for a match against the wireless client's MAC address to determine whether the station is to be allowed or denied to access the network.

To Enable RADIUS Server:

Server IP: The IP address of the RADIUS server.

Port Number: The port number that your RADIUS server uses for authentication. The default setting is 1812.

RADIUS Type: RADIUS

Shared Secret: This is used by your RADIUS server in the Shared Secret field in RADIUS protocol messages. The shared secret configured in the WHA-5500CPE must match the shared secret configured in the RADIUS server. The shared secret can contain up to 64

alphanumeric characters.

RADIUS Server Reattempt Period: The number of times the WHA-5500CPE should attempt to contact the primary server before giving up

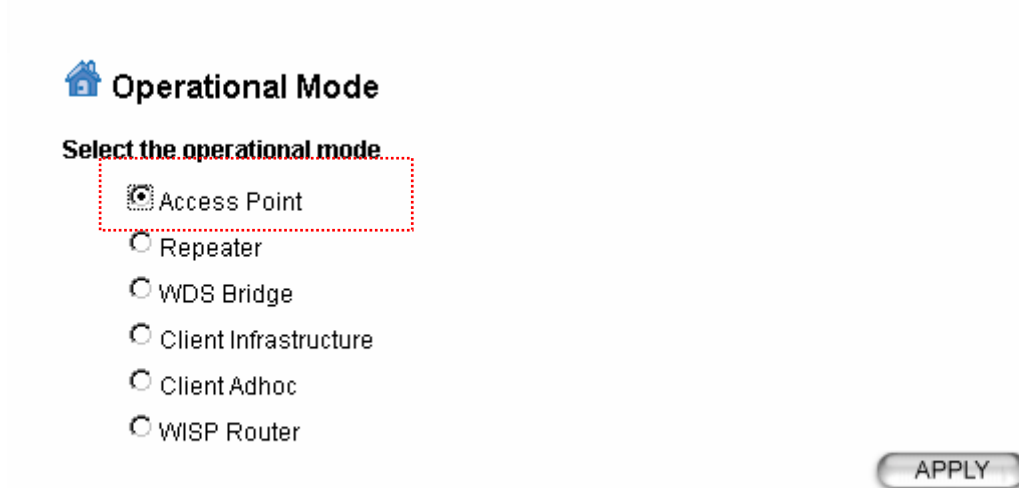
Enter the information for a second RADIUS server in case that there are 2 on your network which you are using to authenticate wireless clients.

3.4 Repeater Mode Settings

For the Repeater node, please be aware that current Repeater mode ONLY works with WHA-5500CPE device as AP node.

3.4.1 AP Node Settings

[Advanced Settings](#)>> [Operational Mode](#)



Operational Mode

Select the operational mode

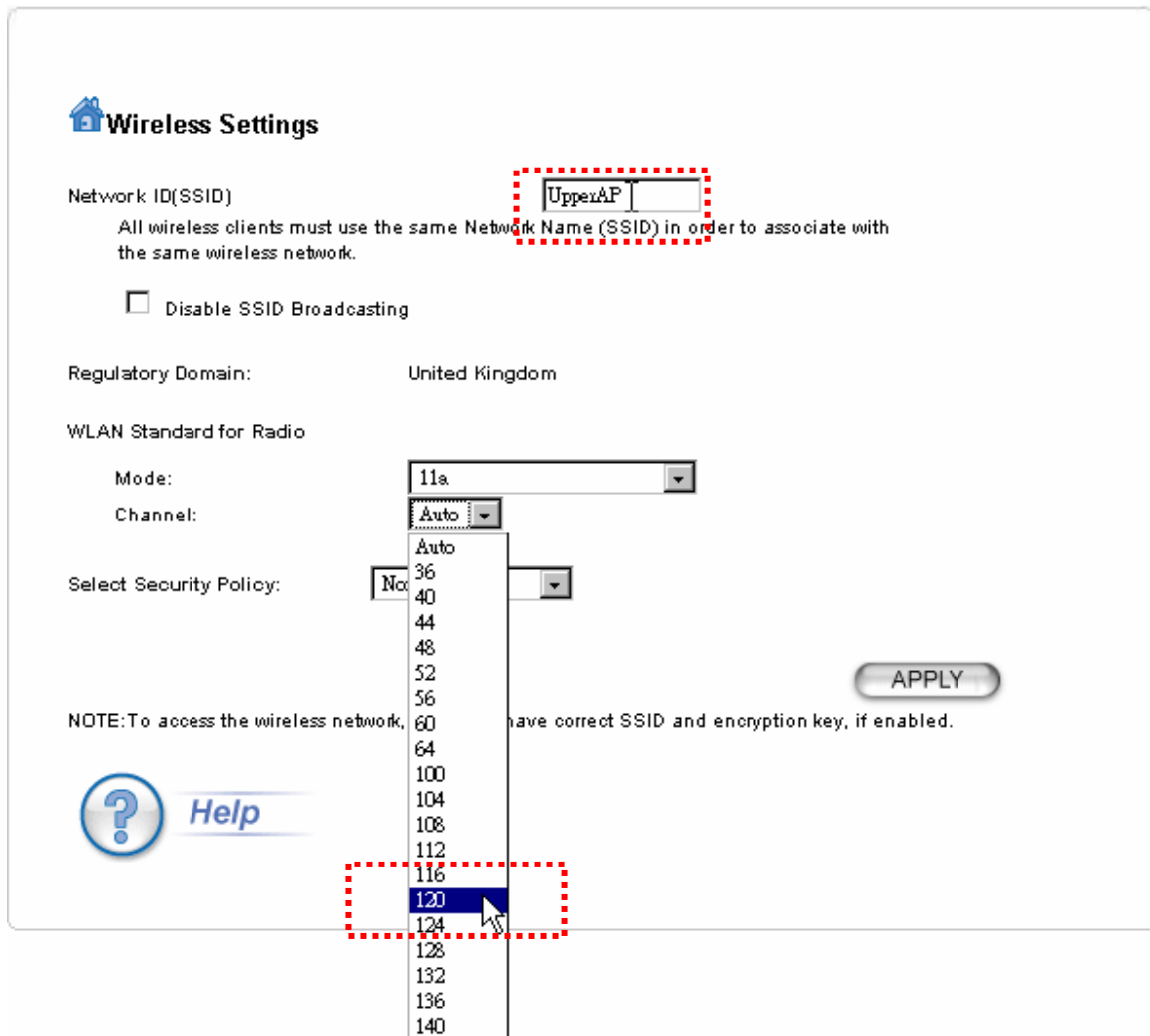
- ☒ Access Point
- ☐ Repeater
- ☐ WDS Bridge
- ☐ Client Infrastructure
- ☐ Client Adhoc
- ☐ WISP Router

APPLY

Set up first the device as an AP mode, click on “APPLY”, Next Step, choose Wireless Mode and channel in the “Wireless Settings” under Setup Wizard.

3. Basic Configuration

Setup Wizard>>Wireless settings



The image shows a 'Wireless Settings' configuration window. At the top, there is a home icon and the title 'Wireless Settings'. Below this, the 'Network ID(SSID)' field is set to 'UpperAP' and is highlighted with a red dashed box. A note states: 'All wireless clients must use the same Network Name (SSID) in order to associate with the same wireless network.' Below the SSID field is a checkbox labeled 'Disable SSID Broadcasting' which is currently unchecked. The 'Regulatory Domain' is set to 'United Kingdom'. Under 'WLAN Standard for Radio', the 'Mode' is set to '11a' and the 'Channel' is set to 'Auto'. A dropdown menu for the channel is open, showing a list of channels from 36 to 140, with '120' selected and highlighted by a red dashed box. The 'Select Security Policy' dropdown is set to 'No'. An 'APPLY' button is located on the right side. At the bottom left, there is a 'Help' button with a question mark icon. A note at the bottom states: 'NOTE: To access the wireless network, you must have correct SSID and encryption key, if enabled.'

Wireless Settings

Network ID(SSID):

All wireless clients must use the same Network Name (SSID) in order to associate with the same wireless network.

☐ Disable SSID Broadcasting

Regulatory Domain: United Kingdom


WLAN Standard for Radio

Mode: 11a

Channel: Auto

Select Security Policy: No

NOTE: To access the wireless network, you must have correct SSID and encryption key, if enabled.

 [Help](#)

APPLY

Select the WLAN mode and channel of your choice
Click on “APPLY” to finish setup.

3.4.2 Repeater Node Settings

[Advanced Settings](#)>>>[Operation Mode](#)

To set a device as Repeater, the device has to be first defined as repeater operation mode.

Operational Mode

Select the operational mode

☐ Access Point
☒ Repeater
☐ WDS Bridge
☐ Client Infrastructure
☐ Client Adhoc
☐ WISP Router

APPLY

Additional configurations for WDS repeater mode:

Remote SSID:

Help

Select “Repeater” mode and then enter the “Remote SSID”, this is the SSID of AP node’s SSID.

Click on the “Repeater” radio button

Key-in the SSID of upper node’s SSID.

Click **APPLY** button.

Next step is to set the AP configuration for client device for Repeater node.

3.4.3 Repeater Node Local service Settings

Setup Wizard>>Wireless Settings

In the Setup Wizard, select the WLAN mode, in this case, only the WLAN mode and SSID can be modified, the channel will automatically readjusted as the upper node.

Wireless Settings

Network ID(SSID):

All wireless clients must use the same Network Name (SSID) in order to associate with the same wireless network.

Regulatory Domain:

WLAN Standard for Radio

Mode:

Channel:

Select Security Policy:

NOTE: To access the wireless network, you must select SSID and encryption key, if enabled.

APPLY

Help

Set the SSID for the Hotspot service. This SSID can be different from upper node's SSID. Its Channel will be display as "Auto" it will be same as the AP node's channel. It's necessary to set the Wireless mode as the same spectrum as AP's node. You can set encryption for the security between hotspot services with client device.

3.4.4 Repeater Advance Wireless Setting

Advanced Settings>>Wireless setting

Beacon Interval: The WHA-5500CPE broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

RTS Threshold: RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it

will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

DTIM Interval: The WHA-5500CPE buffers packets for stations that operate in the power-saving mode. The Delivery Traffic Indication Message (DTIM) informs such power-conserving stations that there are packets waiting to be received by them. The DTIM interval specifies how often the beacon frame should contain DTIMs. It should have a value between 1 to 255, with a default value of **3**.

User Limitation: The range of user limitation is from 1 to 100.

Age Out Timer: Set the age out time. The default is 300 sec.

Transmit Power: Transmit power output depends upon the size and RF characteristics because that will determine the number of APs, channels, and need for antennas.


Ack TimeOut (11a): The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to [Section 3.9](#).

Enable Radio eXtended Range: Select the check box to enable the Atheros's eXtended Range(XR) technology to extend the wireless coverage range.

Enable privacy separator: Select the check box to prohibit data transmission between client stations.

3.4.5 QoS Settings

[Advanced Setting >> QoS Settings](#)


QoS Settings


☒ **Enable WMM**

WMM Parameters of Access Point

AC TYPE	ECWMin	ECWMax	AIFS	TxopLimit-11b(μs)	TxopLimit-11ag(μs)	ACMAck-policy
AC_BE(0)	4	6	3	0	0	<input type="checkbox"/> <input type="checkbox"/>
AC_BK(1)	4	10	7	0	0	<input type="checkbox"/> <input type="checkbox"/>
AC_VI(2)	3	4	1	6016	3008	<input type="checkbox"/> <input type="checkbox"/>
AC_VO(3)	2	3	1	3264	1504	<input type="checkbox"/> <input type="checkbox"/>

WMM Parameters of Station

AC TYPE	ECWMin	ECWMax	AIFS	TxopLimit-11b(μs)	TxopLimit-11ag(μs)	ACMAck-policy
AC_BE(0)	4	10	3	0	0	<input type="checkbox"/>
AC_BK(1)	4	10	7	0	0	<input type="checkbox"/>
AC_VI(2)	3	4	2	6016	3008	<input type="checkbox"/>
AC_VO(3)	2	3	2	3264	1504	<input type="checkbox"/>


[Help](#)

QoS stands for Quality of Service which attempts to provide different levels of quality to different types of network traffic.


QoS stands for Quality of Service which attempts to provide different levels of quality to different types of network traffic.

WMM stands for Wi-Fi Multimedia. WMM defines quality of service ([QoS](#)) in wireless networks. WMM improves audio, video and voice applications transmitted over wireless networks. WMM adds prioritized capabilities to wireless networks and optimizes the performance when multiple concurring applications.

To **Enable WMM**, WMM Parameters of Access Point and Station are indicated. The following information is listed: AC TYPE (AC_BE; Best Effort) (AC_BK; Background)(AC_VI; Video)(AC_VO;Voice)/ ECWMin/ ECWMax/ AIFS/ TxopLimit (11b)/ TxopLimit (11ag)ACM and Ack-policy.

3.4.6 RADIUS Settings

[Advanced Setting >> RADIUS Settings](#)


RADIUS Settings

RADIUS Server

☐ Enable RADIUS Server

Server IP:

0

.

0

.

0

.

0

Port Number:

1812

RADIUS Type:

RADIUS

Shared Secret:

Secondary RADIUS Server

☐ Enable RADIUS Server

Server IP:

0

.

0

.

0

.

0

Port Number:

1812

RADIUS Type:

RADIUS


Shared Secret:

RADIUS Server Reattempt Period

60

Seconds

APPLY


[Help](#)

RADIUS servers provide centralized authentication services to wireless clients. Two RADIUS servers can be defined: one acts as a primary, and the other acts as a backup.

MAC address filtering based authentication requires a MAC address filter table to be created in either the WHA-5500CPE (as described in Chapter 3.2.3 MAC Filtering Settings) and/or the RADIUS server. During the authentication phase of a wireless station, the MAC address filter table is searched for a match against the wireless client's MAC address to determine whether the station is to be allowed or denied to access the network.

To Enable RADIUS Server:

Server IP: The IP address of the RADIUS server.

Port Number: The port number that your RADIUS server uses for authentication. The default setting is 1812.

RADIUS Type: RADIUS

Shared Secret: This is used by your RADIUS server in the Shared Secret field in RADIUS protocol messages. The shared secret configured in the WHA-5500CPE must match the shared secret configured in the RADIUS server. The shared secret can contain up to 64

alphanumeric characters.

RADIUS Server Reattempt Period: The number of times the WHA-5500CPE should attempt to contact the primary server before giving up

Enter the information for a second RADIUS server in case that there are 2 on your network which you are using to authenticate wireless clients.

3.5 WDS Bridge Mode Settings

[Advanced Setting >> Operation Mode>> WDS Bridge](#)

Select “WDS Bridge” mode and then press the ‘APPLY’ button. Additionally, to use the WDS as AP-client mode with SSID, please choose “Infrastructure Mode” radio button.

Select the operational mode

- ☐ Access Point
☐ Repeater
☒ WDS Bridge
☐ Client Infrastructure
☐ Client Adhoc
☐ WISP Router

APPLY

Additional configurations for WDS bridge mode:

Name:

MAC address: -----

Select Security Policy:

None ▼

ADD

Select	Name	MAC Address	Security
-	-	-	-

DELETE SELECTED

When configured as a WDS Bridge Pure MAC mode, you need to further configure the name and MAC address of its peer WDS devices.

3.5.1 Wireless Settings

[Advanced Setting >> Wireless Setting](#)

Beacon Interval : msec. (range: 20-1000, default 100)
RTS Threshold : bytes (range: 0-2347, default 2347)
Fragmentation : bytes (range: 256-2346, default 2346)
DTIM Interval : (range 1-255, default 1)
User Limitation: (range: 1-100, default 100)
Age Out Timer : (min. range: 1-1000, default 5)
Transmit Power: (Reduce Tx Power between 0~14 dB)
Rate Control: Mbps
AckTimeOut (11a/SuperA): μ s (range: 10-255, default 25)

☐ **Enable Radio eXtended Range**
☐ **Enable privacy separator**
☐ **Enable STP**
☒ **Enable 802.11d**

RTS Threshold: RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

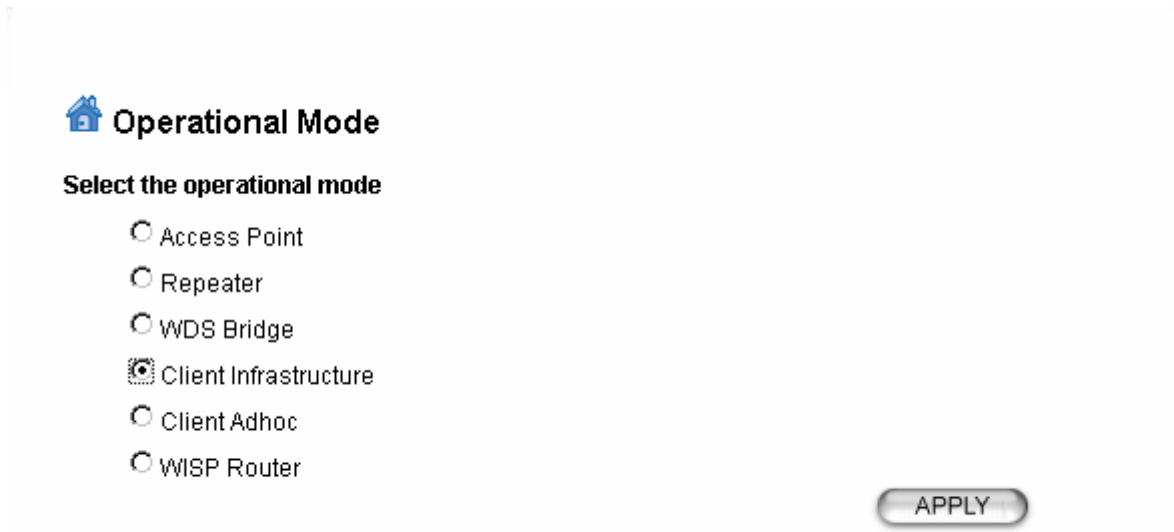
Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

Transmit Power: Transmit power output depends upon the size and RF characteristics because that will determine the number of APs, channels, and need for antennas.

Ack TimeOut (11a): The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to [Section 3.9](#).

3.6 Client Infrastructure Mode Settings

[Advanced Setting>>Operation Mode>> Client Infrastructure](#)



Operational Mode

Select the operational mode

- ☐ Access Point
- ☐ Repeater
- ☐ WDS Bridge
- ☒ Client Infrastructure
- ☐ Client Adhoc
- ☐ WISP Router

APPLY

Select “Client Infrastructure” mode and then click APPLY button.

The client can search for the SSIDs of APs in the environment, in order to select the AP that he wants to make connection with. For details, please go to Section 4.5: [Device Status>>Site Survey](#)

3.6.1 Wireless Settings

[Advanced Setting >> Wireless Setting](#)

Wireless Settings

RTS Threshold : bytes (range: 0-2347, default 2347)

Fragmentation : bytes (range: 256-2346, default 2346)

Transmit Power: (Reduce Tx Power between 0~14 dB)

AckTimeOut (11a/SuperA): μ s(range: 10-255, default 25)

[ACK Calculator](#)

RTS Threshold: RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

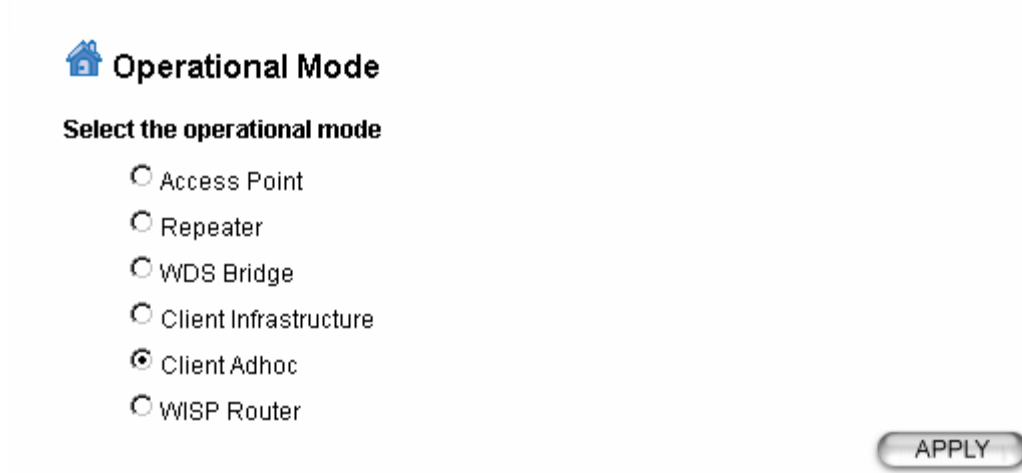
Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

Transmit Power: Transmit power output depends upon the size and RF characteristics because that will determine the number of APs, channels, and need for antennas.

Ack TimeOut (11a): The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to [Section 3.9](#).

3.7 Client Adhoc Mode Settings

[Advanced Setting >> Operation Mode >> Client Adhoc](#)



Operational Mode

Select the operational mode

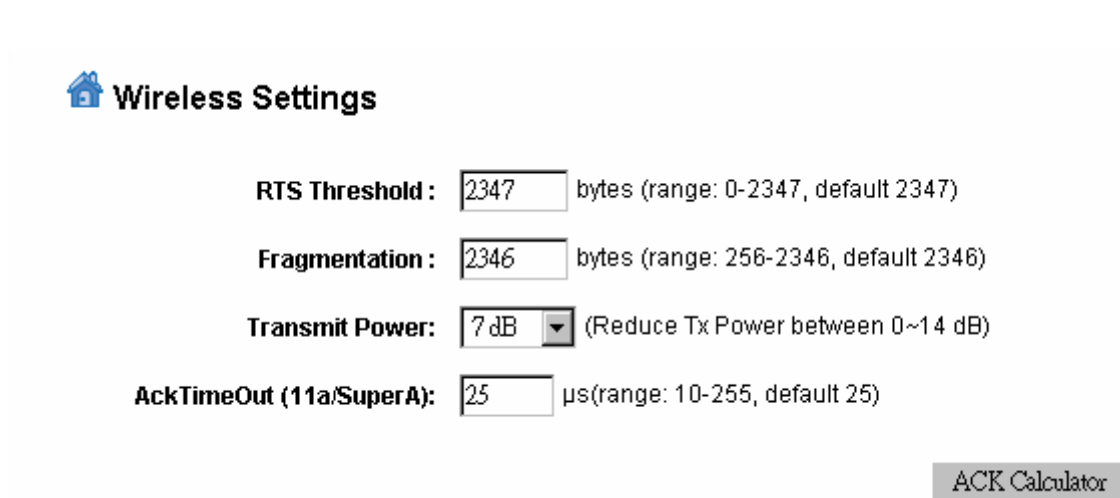
☐ Access Point
☐ Repeater
☐ WDS Bridge
☐ Client Infrastructure
☒ Client Adhoc
☐ WISP Router

APPLY

Select “Client Adhoc” mode and then click APPLY button.

3.7.1 Wireless Settings

[Advanced Setting >> Wireless Settings](#)



Wireless Settings

RTS Threshold: bytes (range: 0-2347, default 2347)

Fragmentation: bytes (range: 256-2346, default 2346)

Transmit Power: (Reduce Tx Power between 0~14 dB)

AckTimeOut (11a/SuperA): μ s (range: 10-255, default 25)

ACK Calculator

RTS Threshold: RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

Transmit Power: Transmit power output depends upon the size and RF characteristics because that will determine the number of APs, channels, and need for antennas.

Ack TimeOut (11a): The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to [Section 3.9](#).

3.8 WISP Router Mode Settings

[Advanced Setting >> Operation Mode >> WISP Router](#)

Operational Mode

Select the operational mode

- ☐ Access Point
- ☐ Repeater
- ☐ WDS Bridge
- ☐ Client Infrastructure
- ☐ Client Adhoc
- ☒ WISP Router

APPLY

Select "WISP Router" mode and then click APPLY button.

3.8.1 Wireless Settings

[Advanced Setting >> Wireless Settings](#)

Wireless Settings

RTS Threshold: bytes (range: 0-2347, default 2347)

Fragmentation: bytes (range: 256-2346, default 2346)

Transmit Power: (Reduce Tx Power between 0~14 dB)

AckTimeOut (11a/SuperA): μ s (range: 10-255, default 25)

ACK Calculator

APPLY

RTS Threshold: RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold

should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.


Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of **2346**. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

Transmit Power: Transmit power output depends upon the size and RF characteristics because that will determine the number of APs, channels, and need for antennas.

Ack TimeOut (11a): The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. For details, please go to [Section 3.9](#).

3.8.2 WISP Router DHCP Server Settings

[Advanced Setting >> DHCP server Setting](#)

 **DHCP Server Settings**

☒ **Enable DHCP Server**

Assigns IP addresses to wired and wireless clients from the following range:

Lease Time: seconds

From: . . .


To: . . .

Assigns the following IP address to the client with the following MAC address:

MAC Address: - - - - -

IP Address: . . .

Select	IP Address	MAC Address
-	-	-

 [Help](#)

DHCP stands for Dynamic Host Configuration Protocol. The DHCP server dynamically assigns IP addresses (from a pre-defined list) to clients when they log on. The client will request a new IP when the specific period of time is about to run out. If it expires, the address is returned to the pool of IP addresses.


Under WISP mode, select the check box of “Enable DHCP Server” to enable DHCP server function.

The range of Clients’ IP addresses is from 192.168.1.2 to 192.168.1.254.

You can assign an IP address to a specified MAC address.

3.8.3 Multiple DMZ

[Advanced Settings >> Multiple DMZ](#)

 **Multiple DMZ**

Select a DMZ type: ☒ Default DMZ ☐ Multiple DMZ

Local DMZ IP address: . . .

ADD

Select	Name	Public WAN IP	Local DMZ IP
-	-	-	-

DELETE SELECTED


NOTE: A DMZ server is a common term used to describe the default virtual server. If the DMZ server is selected, Internet traffic not destined for a valid virtual server is redirected to this privately-addressed LAN client. This can be used together with a separate firewall device to perform additional security functions.

Select a DMZ type and then enter the local DMZ IP address.

Note: A DMZ server is a common term used to describe the default virtual server. If the DMZ server is selected, Internet traffic not destined for a valid virtual server is redirected to this privately addressed LAN client. This can be used together with a separate firewall device to perform additional security functions.

3.8.4 Virtual Server Settings

[Advanced Settings >> Virtual Setting](#)


Virtual Server Settings

This allows you to specify one or more applications running on server computers on the LAN that may be accessed by any Internet user. Internet data destined for the specified public port will be directed to the specified private port number on the LAN client with the specified private IP address.

Service Name:


Public Port No.: ☒ Single

☐ Range ~

Local IP Address: . . .

Local Port No. Starts From:

Select	Service	Public Port No(s)	Local IP Address	Local Port No(s)
-	-	-	-	-


Help

This allows you to specify one or more applications running on server computers on the LAN that may be accessed by any Internet user. Internet data destined for the specified public port will be directed to the specified private port number on the LAN client with the specified private IP address.

3.8.5 Special Applications

[Advanced Setting >> Special Applications](#)

Special Applications

Some Internet applications such as Instant Messaging or Games in particular use groups of ports, and are not easy to work behind a firewall. To work well with these special applications we will open ports to let traffic pass through. Before you set up special application, please see your applications' help for such information.

Select an Application:

Name:

Trigger Ports:

Trigger Protocol:

Opened Ports: ~

Opened Protocol:

ADD

Select	Name	Trigger Port	Trigger Protocol	Opened Ports	Opened Protocol
-	-	-	-	-	-

DELETE SELECTED

NOTE: You can use up to 3 sets of opened ports for a specific application. The opened ports can be separated by a comma and no spaces are allowed (e.g. 2300-2305,4300-4305,5300-5305).

Some Internet application such as Instant Messaging or Games in particular use groups of ports, and are not easy to work behind a firewall. To work well with these special applications we will open ports to let traffic pass through.

Note: You can use up to 3 sets of opened ports for a specific application. The opened ports can be separated by a comma and no spaces are allowed (e.g. 2300-2305, 4300-4305, 5300-5305).

3.8.6 IP Filtering Settings

[Advanced Setting>>IP Filtering Settings](#)

IP filtering is simply a mechanism that decides which types of IP datagrams will be processed normally and which will be discarded.

IP Filtering Settings

This allows you to define rules for allowing / denying access from / to the Internet.

- ☒ **Disable IP filtering**
No IP filtering is performed.
- ☐ **Grant IP access**
Data traffic satisfying rules below are allowed/forwarded.
- ☐ **Deny IP access**
Data traffic satisfying rules below are denied/filtered.

APPLY

Define an IP filtering rule:

Name:

IP Protocol:

Apply to : ☒ Outbound to the Internet ☐ Inbound from the Internet

Source IP Address: ☒ Any

☐ Single IP

☐ Network

IP: . . .

Netmask: . . .

Dest. IP Address: ☒ Any

☐ Single IP

☐ Network

IP: . . .

Netmask: . . .

ADD

Select	Name	IP Protocol	Apply to	Source IP Address(es)	Source Port(s)	Dest. IP Address(es)	Dest. Port(s)
-	-	-	-	-	-	-	-

DELETE SELECTED

NOTE: Incorrect configuration may cause undesirable behavior. Please refer to the user manual for more details.



This allows you to define rules for allowing / denying access from / to the Internet.

Please do set both inbound/outbound in order to get complete connection. Only inbound or outbound will not allow to get response from the destination IP.

Disable IP filtering: No IP filtering is performed.

Grant IP access: Data traffic satisfying rules below are allowed/forwarded.

Deny IP access: Data traffic satisfying rules below are denied/filtered.


You can also define IP filtering rule, such as:

Name; IP Protocol; Apply to either Outbound to the Internet or Inbound from the Internet; Source IP Address and Dest. (Destination) IP Address.

To grant or deny IP address, select **ADD** or **Delete Selected**.

3.8.7 IP Routing Settings

[Advanced Setting >> IP Routing Settings](#)

 **IP Routing Settings**

Dynamic Routing

Select the routing protocol scheme used for the router's LAN / WAN port.

☒ **Disable**
☐ **RIP**

APPLY

Static Routing

This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.

Destination IP Address: . . .
 Subnet Mask: . . .
☒ Gateway IP Address: . . .
☐ Interface:
 Metric Count:

ADD

To add a static route, enter the information above and click **ADD**.


IP Routing Table

Select	Destination IP Address	Subnet Mask	Gateway IP Address	Interface	Flag	Metric
-	192.168.1.0	255.255.255.0	-	lan	U	0
-	239.0.0.0	255.0.0.0	-	lan	U	0

DELETE SELECTED

To delete a static route from the table, select the route and click **DELETE SELECTED**.

NOTE: Changes to the routing table will take effect immediately.

 [Help](#)

Dynamic Routing:

Select the routing protocol scheme used for the router's LAN / WAN port.

Static Routing:

This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.

IP Routing Table:

To delete a static route from the table, select the route and click DELETE SELECTED.

Note: Changes to the routing table will take effect immediately.

3.9 ACK Timeout Setup

Ack TimeOut (11a): The "ACK time-out" determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file. WHA-5500CPE provides a calculator on UI that helps you to obtain this value only by giving the distance.

Wireless Settings

RTS Threshold : bytes (range: 0-2347, default 2347)

Fragmentation : bytes (range: 256-2346, default 2346)

Transmit Power: (Reduce Tx Power between 0~14 dB)

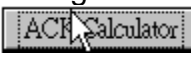
AckTimeOut (11a/SuperA): μ s (range: 10-255, default 25)

ACK Calculator

Input distance value in meters. The ACK Timeout value will be automatically calculated accordingly. This is the value to be entered into the "ACK Timeout (11a)" field according to the spectrum.

ACK Calculator

Advanced setting >> wireless settings

Click on the "ACK Calculator"  at the right down side of this page.

802.11a ACK Calculator

(The result is for your reference only, it can vary by +/- 15)

Distance: m.

Ack:

AckTimeOut:

In the field of "Distance", input the distance in "meters".

After input the distance value, move the cursor to any place on the pop-up window out of three fields. The calculated value will display.

802.11a ACK Calculator

(The result is for your reference only, it can vary by +/- 15)

Distance: m.

Ack:

AckTimeOut:



Enter the calculated value of “AckTimeOut” into the appropriate “Ack TimeOut” field (11a) in the “Wireless Settings” window.

Wireless Settings

RTS Threshold : bytes (range: 0-2347, default 2347)

Fragmentation : bytes (range: 256-2346, default 2346)

Transmit Power: (Reduce Tx Power between 0~14 dB)

AckTimeOut (11a): (range: 10-255, default 25)

ACK Calculator

APPLY

4

Manage the WHA-5500CPE

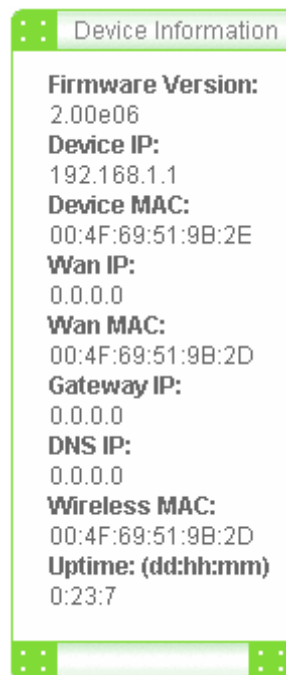
This Chapter covers other management aspects of your WHA-5500CPE:

- Check Device Information
- View System Log
- Wireless Client Table
- Radio Table
- Site Survey
- Upgrade Firmware
- Save or Restore Configuration Changes
- Reset to Factory Default
- Reboot AP
- What if you forgot the password?

4.1 Device Status

[Device status >> Device Information](#)

You can monitor the system status and get general device information from the **Device Information** screen:



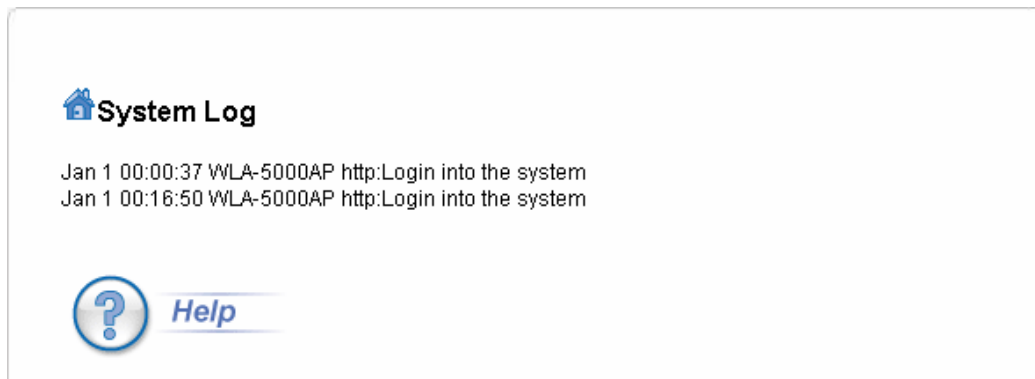
This is at the left-bottom corner of the **Device Status** window.

4.2 System Log

[Device Status >> System Log](#)

The WHA-5500CPE maintains a system log that you can use to track events that have occurred in the system. Such event messages can sometimes be helpful in determining the cause of a problem that you may have encountered.

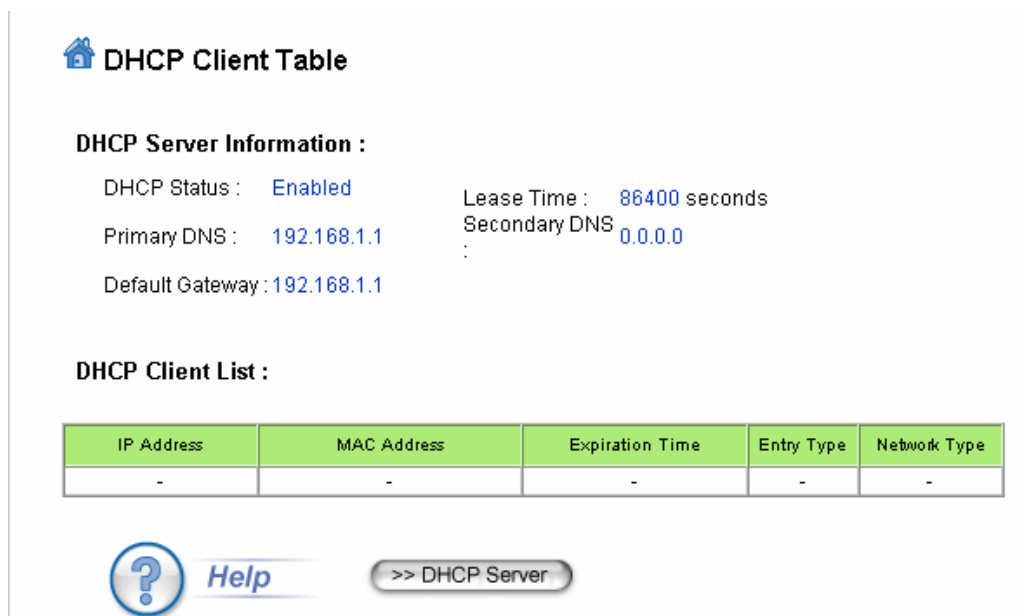
You can select **System Log** on the left side of the **Device Status** window to view log events recorded in the system. The System Log entries are shown in the main screen along with the log level, the severity level of messages that are being displayed (lower is severer), and the uptime, which is the amount of time since the WHA-5500CPE was boot-up.



4.3 Wireless Client Table

[Device Status >> Wireless Client Table](#)

The wireless client table lists the current wireless clients and its MAC address, state, and traffic statistics. You can check this table by clicking **Wireless Client Table** at the left side of the **Device Status** window.

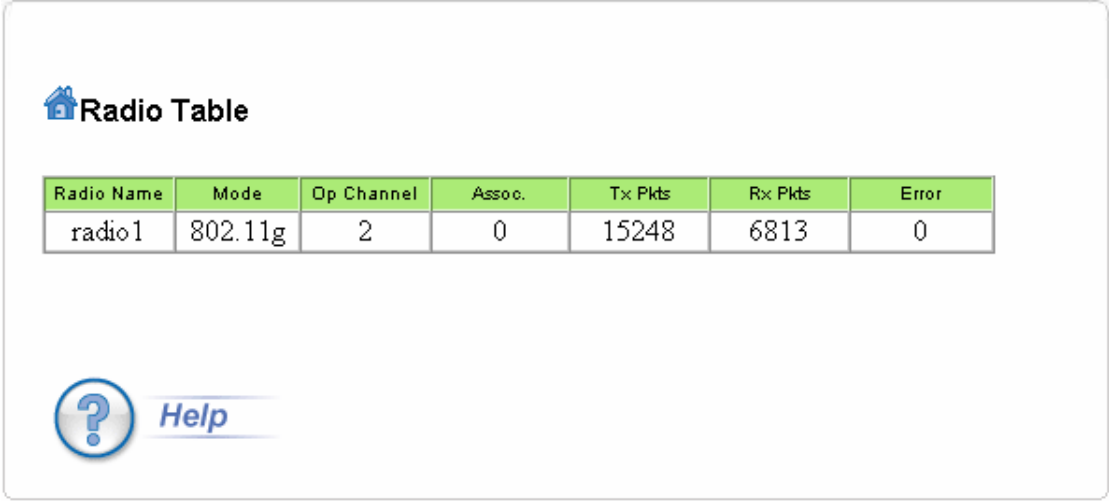


4.4 Radio Table

[Device Status >> Radio Table](#)

The Radio Table indicates wireless radio counters' data under one of the six operational modes: Access Point; Repeater; WDS Bridge; Client Infrastructure, Client Adhoc and WISP Router.

Radio Table will indicate the following information: Radio Name, Mode, Op Channel, Assoc. Tx Pkts, Rx Pkts and Error.



The screenshot shows a web interface titled "Radio Table" with a home icon. Below the title is a table with 7 columns: Radio Name, Mode, Op Channel, Assoc., Tx Pkts, Rx Pkts, and Error. The table contains one row of data for "radio1". Below the table is a help icon (a question mark in a circle) and the word "Help".

Radio Name	Mode	Op Channel	Assoc.	Tx Pkts	Rx Pkts	Error
radio1	802.11g	2	0	15248	6813	0

4.5 Site Survey


[Device Status >> Site Survey](#)

The Site Survey table shows the wireless Access Point and Ad Hoc stations in your environment detected by the 802.11 A/G Access Point. You can click the **REFRESH** button to get latest environment information.

Site Survey list will indicate the following information:
ESSID, MAC Address, Conn Mode, Channel, Turbo, Super, XR, WME, Signal strength (%), Security and Network


The Site Survey table is available for only the following operation modes:

- (1) Access Point
- (2) Repeater
- (3) Client Infrastructure
- (4) Client Adhoc
- (5) WISP Router

 **Site survey**

Site survey list :

	ESSID	MAC Address	Conn Mode	Channel	Turbo	Super	XR	WME	Signal Strength(dbm)	Security	Network
<input type="radio"/>	Default_WLAN	00:06:4f:53:e7:b1	G	1	-	-	-	-	-71	None	AP
<input type="radio"/>	airlivewps	00:c0:a8:ea:e3:17	G	2	-	*	-	-	-92	WEP	AP
<input type="radio"/>	WAP-4035	00:30:4f:42:0b:d0	G	10	-	-	-	-	-35	WEP	AP


 [Help](#) ASSOCIATE REFRESH SIGNAL SURVEY

4.5.1 Signal survey

[Device Status >> Site Survey >> Signal Survey](#)


This is a unique feature from AirLive. It provides real-time signal strength between two nodes. Better signal strength means better alignment results, which aims to improve link quality.

Click the “SIGNAL SURVEY” button. A pop-up window will continuously display signal strength in real time. The user can readjust the antenna position in order to achieve maximum signal strength.

 **Site survey**

Site survey list :

	ESSID	MAC Address	Conn Mode	Channel	Turbo	Super	XR	WME	Signal Strength(dbm)	Security	Network
<input type="radio"/>	Default_WLAN	00:06:4f:53:e7:b1	G	1	-	-	-	-	-71	None	AP
<input checked="" type="radio"/>	airlivewps	00:c0:a8:ea:e3:17	G	2	-	*	-	-	-92	WEP	AP
<input type="radio"/>	WAP-4035	00:30:4f:42:0b:d0	G	10	-	-	-	-	-35	WEP	AP

 [Help](#) ASSOCIATE REFRESH SIGNAL SURVEY

http://192.168.1.1 - Signal Strength - Mozilla Firefox

BSSID: - - - - -

Channel:

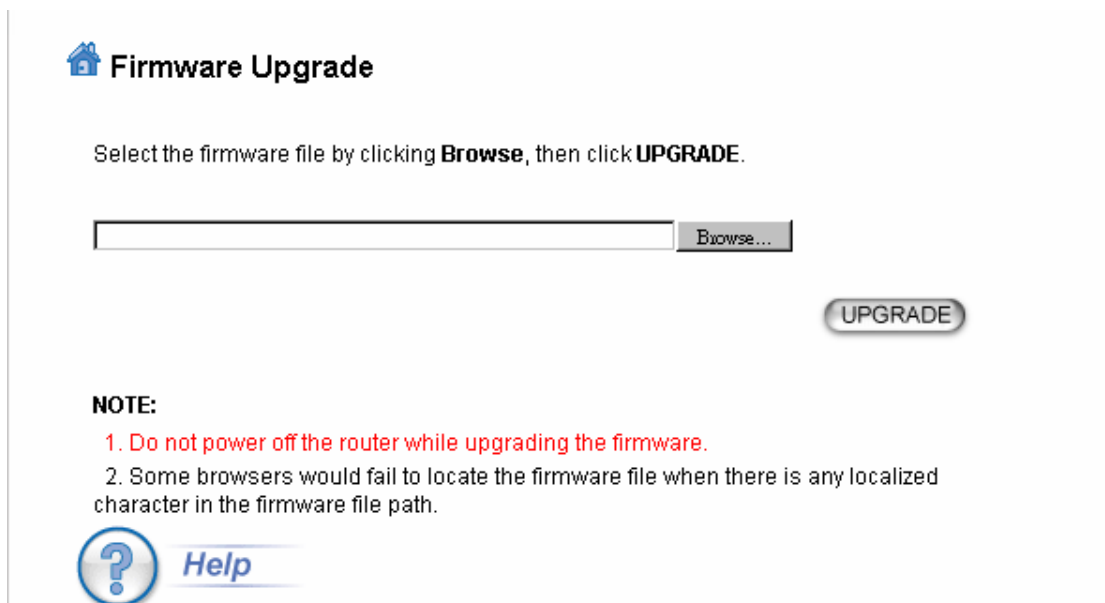
Signal Strength: dbm

4.6 Firmware Upgrade

System tools >> Firmware Upgrade

You can upgrade the firmware of your WHA-5500CPE (the software that controls your WHA-5500CPE's operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems that you have encountered with the current version. System upgrade can be performed through the System Upgrade window as follows:

Step 1 Select **System Tools**, then **Firmware Upgrade** from the menu.



Firmware Upgrade


Select the firmware file by clicking **Browse**, then click **UPGRADE**.

Browse...

UPGRADE

NOTE:

1. Do not power off the router while upgrading the firmware.
2. Some browsers would fail to locate the firmware file when there is any localized character in the firmware file path.

 **Help**

Step 2 To update the WHA-5500CPE firmware, first download the firmware from the distributor's web site to your local disk, and then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Upgrade** button to start.

The new firmware will be loaded to your WHA-5500CPE. After a message appears telling you that the operation is completed, you need to reset the system to have the new firmware take effect.



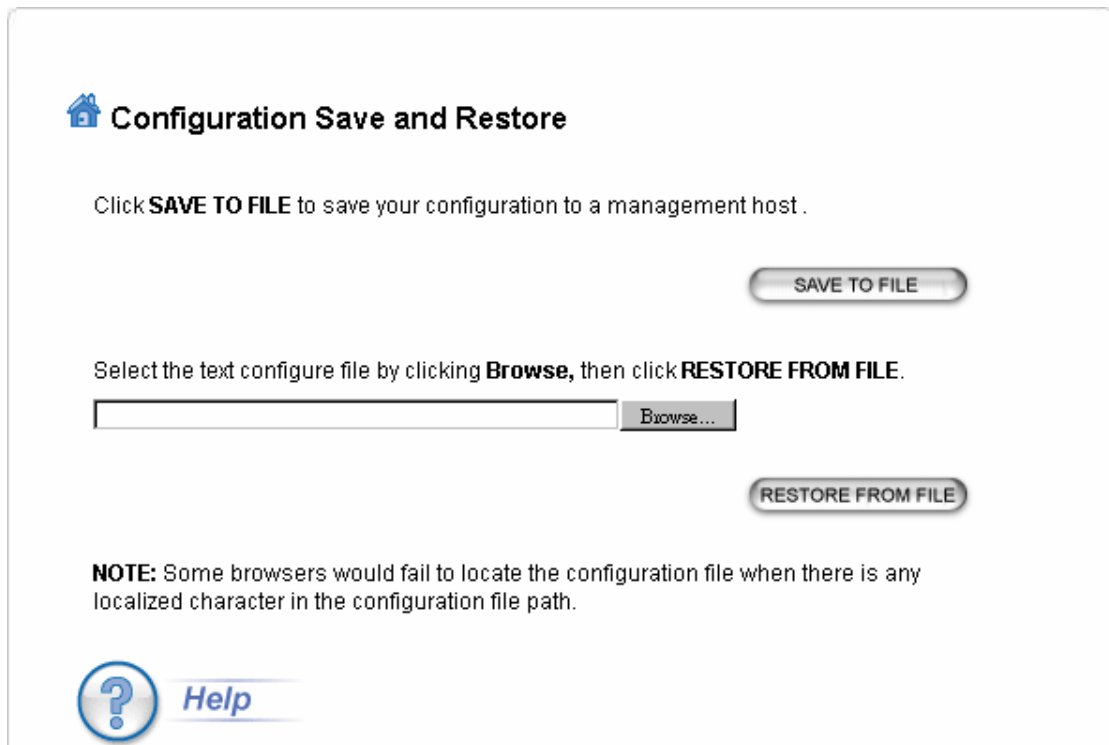
Do not power off the device while upgrading the firmware. It is recommended that you do not upgrade your WHA-5500CPE unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

4.7 Configuration Save and Restore

System Tools >> Configuration Save and Restore

You can save system configuration settings to a file, and later download it back to the WHA-5500CPE by following the steps.

Step 1 Select **Configuration Save and Restore** from the **System Tools** menu.



The screenshot shows a web interface titled "Configuration Save and Restore" with a home icon. It contains the following elements:

- A text instruction: "Click **SAVE TO FILE** to save your configuration to a management host."
- A button labeled "SAVE TO FILE".
- A text instruction: "Select the text configure file by clicking **Browse**, then click **RESTORE FROM FILE**."
- A text input field followed by a "Browse..." button.
- A button labeled "RESTORE FROM FILE".
- A **NOTE**: "Some browsers would fail to locate the configuration file when there is any localized character in the configuration file path."
- A help icon (question mark in a circle) and a "Help" link.

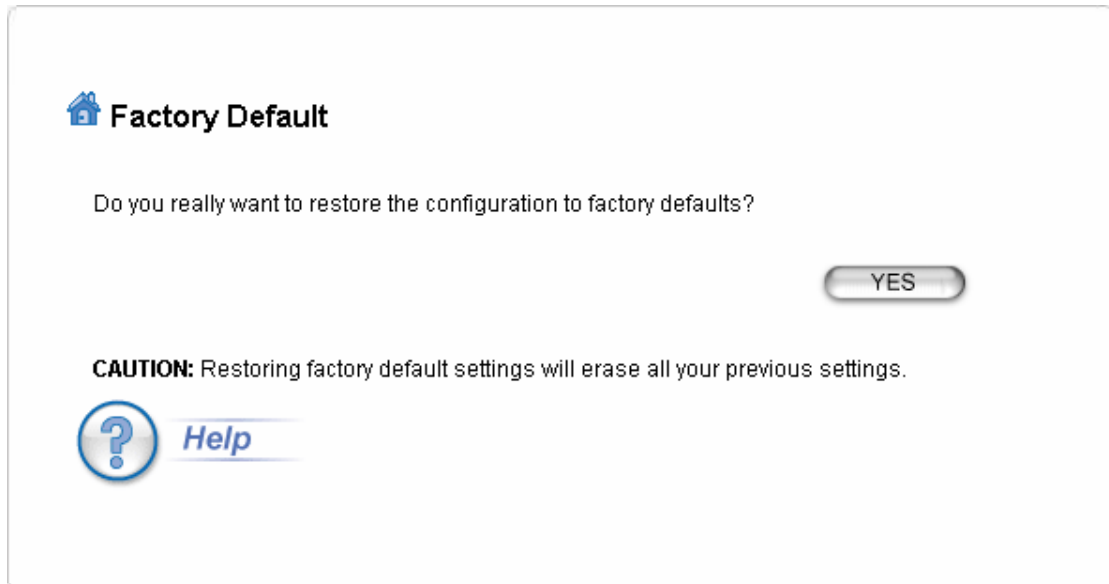
Step 2 Enter the path of the configuration file to save-to/restore-from (or click the **Browse** button to locate the configuration file). Then click the **SAVE TO FILE** button to save the current configuration into the specified file, or click the **RESTORE FROM FILE** button to restore the system configuration from the specified file.

4.8 Factory Default

[System Tools >> Factory Default](#)

You can reset the configuration of your WHA-5500CPE to the factory default settings. To do it:

Step 1 Select **Factory Default** from the **System Tools** menu.



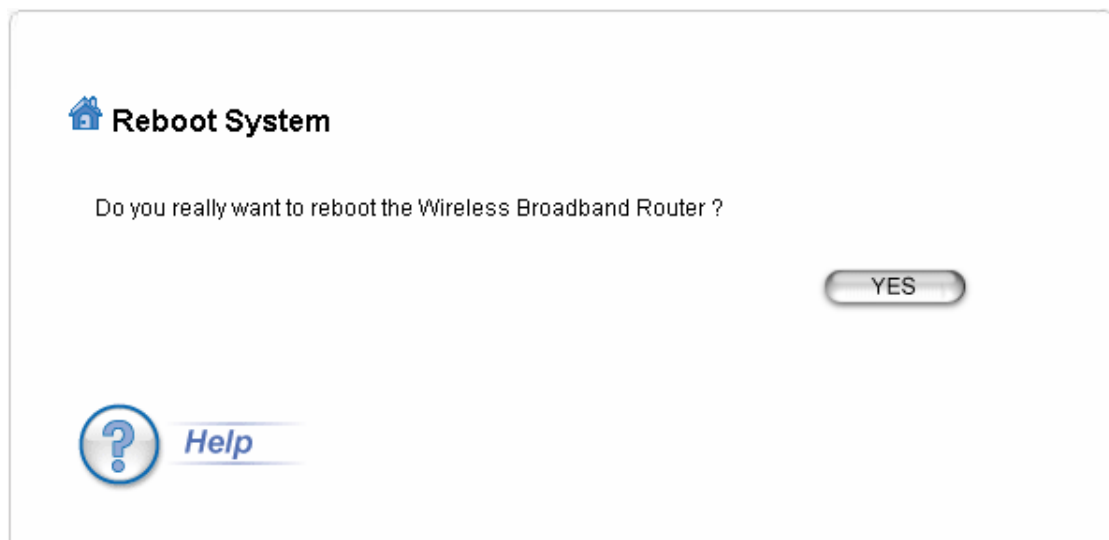
Step 2 Click **YES** to go ahead and restore the configuration to the factory default.

4.9 Reboot System

[System tools>>Reboot System](#)

You can reset your WHA-5500CPE from the Browser. To reset it:

Step 1 Select **Reboot System** from the **System Tools** menu.



Step 2 Click **YES** to reboot the WHA-5500CPE.



Rebooting the WHA-5500CPE would disconnect any active clients and therefore will disrupt any current data traffic.

4.10 What if you forgot the password?

Hardware Reset To Factory Defaults

If you forgot the password, the only way to recover is to clear the device configuration and return the unit to its original state as shipped from the factory.

You can reset the Access Point's Settings to factory defaults by pushing a paperclip in the RESET hole on the PCB panel. Push and hold for around 2 seconds until the lights at the front of the Access Point are off. Doing so will clear your current configuration.

Specifications

AP Specification

Product Name	• IEEE WHA-5500CPE
OS	• Linux® 2.4.18
Standard	<ul style="list-style-type: none"> • IEEE 802.11a • IEEE 802.1d Spanning Tree • IEEE 802.1x • IEEE 802.3u Ethernet protocol
WLAN Network Architecture Type	• Infrastructure
TX-Power (5470-5725MHz)	• 54 Mbps @ 17 dBm
	• 48 Mbps @ 18 dBm
	• 36 Mbps @ 19 dBm
	• 6, 9, 12, 18, 24 Mbps @ 20 dBm
Receiver Sensitivity (Tolerance : max/min= +3/-1.5dB)	• 54Mbps@-71 dBm
	• 12Mbps@-88 dBm
	• 6Mbps@-90 dBm
Wireless Transfer Data Rate for IEEE 802.11a Draft Standard	• IEEE 802.11a Standard: 54, 48, 36, 24, 18, 12, 9 & 6 Mbps with auto fallback
Physical Specification	<ul style="list-style-type: none"> • 802.3af Power over Ethernet with DC48V/0.4A or 5.5V/2.5A power adaptor(optional) • Desktop Installation • Wall Mountable with mounting kits
Hardware & Antenna	<ul style="list-style-type: none"> • 1 x RJ45 • 1 x Restore Button • 1x Integrated Patch Antenna
Security	<ul style="list-style-type: none"> • WEP 64-bit, 128-bit, 152-bit Encryption • MAC Access Control for the wireless interface • EAP & 802.1x support • Support Primary & secondary RADIUS server • WPA and WPA-PSK
Management	<ul style="list-style-type: none"> • Web-Based Management Tool • UPnP • Upload & download test-based configuration file via HTTP browser • Firmware upgrade via HTTP browser • SysLog
IP Address Assignment	<ul style="list-style-type: none"> • DHCP Client • Static IP Address
Dimension	<ul style="list-style-type: none"> • L x W x H : 225mm x 122mm x 225mm • Weight :920 g(without Mounting kit)
Environmental Specification	<ul style="list-style-type: none"> • Operation Temperature: 0°C ~ 40°C. • Storage Temperature: -20°C ~ 65°C • Operating Humidity: 10% ~ 90% (without Condensation)
EMC Certification	• CE

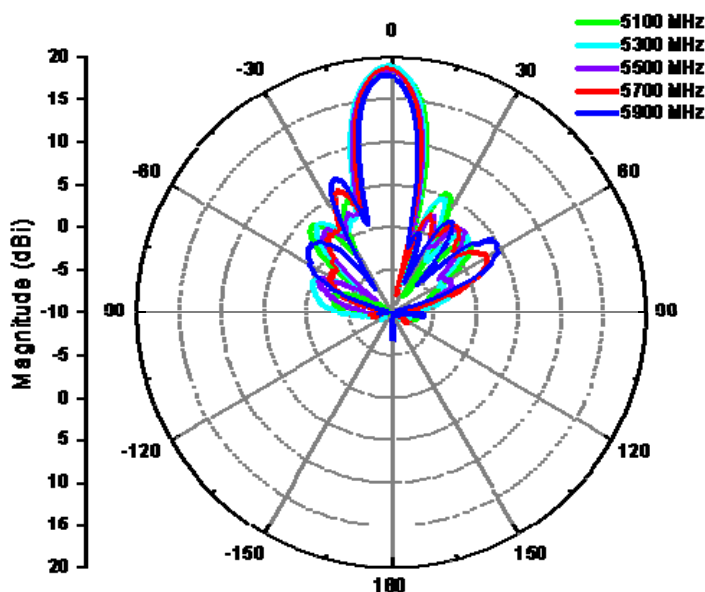
Antenna Specification

Frequency range	• 5150 MHz - 5875 MHz
Gain	• 18 dBi
VSWR	• 2.0 : 1 Max
Polarization*	• Linear, vertical
HPBW/Horizontal	• 13.5° - 15.5°
HPBW/vertical	• 13° - 16°
Front-to-back ratio	• 25 dB
Power handling	• 6 W (cw)
Impedance	• 50 Ohms
Connector	• MMCX
Cable	• RG 316, 15cm
Sidelobe	• ETSI EN 302 085 V1.2.3 Class TS1-TS2
Cross-polarization	• ETSI EN 302 085 V1.2.3 Class TS1-TS2

Environmental & Mechanical Characteristics

Survival wind speed	• 216 km/hr
Temperature	• -40°C to +80°C
Humidity	• 95% @55°C
Lightning protection	• DC ground
Radome color	• Gray-white
Radome material	• PC, UV resistant
Weight	• 870 g
Dimensions	• 225 x 225 x 115 mm

Radiation Pattern: H-plane



Radiation Pattern: V-plane

